



EUROPEAN COMMISSION

DIRECTORATE-GENERAL

Joint Research Centre

APPROACHES TO THE SECURITY ANALYSIS OF POWER SYSTEMS: DEFENCE STRATEGIES AGAINST MALICIOUS THREATS

E. Bompard(*), C. Gao(*), M. Masera(), R. Napoli(*), A.
Russo(*), A. Stefanini(**), F. Xue (*)**

(*) Politecnico di Torino, Department of Electrical Engineering, Corso Duca degli
Abruzzi, 24, 10129 Torino (ITALY), ettore.bompard@polito.it

(**) JRC, Institute for the Protection and Security of the Citizen, Via E. Fermi, 1,
21020 Ispra (VA), Italy marcelo.masera@jrc.it

IPSC

EUR 22683 EN

The mission of the Institute of the Protection and Security of the Citizen of the Joint Research Centre is to provide research-based, system-oriented support to EU policies so as to protect the citizen. The main application areas are cyber-security and the fight against fraud; natural, technological and economic risks; humanitarian security, non-proliferation and nuclear safeguards. The Institute will continue to maintain and develop its expertise in information, communication, space and engineering technologies in support of its mission.

European Commission
Directorate-General Joint Research Centre
Institute IPSC

Contact information
Address: Via E. Fermi, 1 - 21020 Ispra (VA)
E-mail: Marcelo.Masera@jrc.it
Tel.: 0332/789238
Fax: 0332/789576

<http://www.jrc.cec.eu.int>

Legal Notice

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server
<http://europa.eu>

EUR 22683 EN

ISSN 1018-5593

Luxembourg: Office for Official Publications of the European Communities
© European Communities, 2007
Reproduction is authorised provided the source is acknowledged

Printed in Italy

INDEX

1.	FOREWORD	2
2.	INTRODUCTION	2
2.1	GROWING CONCERN FOR THE SECURITY OF CRITICAL INFRASTRUCTURES	3
2.2	CLASSIFICATION OF THREATS TO INFRASTRUCTURES	5
2.3	ACTORS IN CRITICAL INFRASTRUCTURES	7
3.	MALICIOUS ATTACKS AND DEFENCE STRATEGIES	9
3.1	NATURAL VERSUS MALICIOUS THREATS	9
3.2	IMPACT OF ATTACKS AND DEFENCE/ATTACK COST	10
4.	MODELLING OF THE STRATEGIC INTERACTIONS IN MALICIOUS ATTACKS	13
4.1	GAME THEORY APPLICATIONS TO MALICIOUS ATTACKS MODELING	13
4.1.1	DEFINITIONS	13
4.1.2	THE SEARCH FOR AN EQUILIBRIUM	16
4.1.3	APPLICATION OF GAME THEORY TO STRATEGIC INTERACTION IN MALICIOUS ATTACKS TO POWER SYSTEMS	17
4.2	EXAMPLE OF GAME MODEL FOR RISK ANALYSIS IN MALICIOUS ATTACKS	18
4.2.1	MODEL DESCRIPTION	19
4.2.2	CASE STUDY AND RESULTS	22
5.	MODELING OF COORDINATION/COOPERATION UNDER MALICIOUS ATTACKS WITH MAS	29
5.1	MAS APPLICATION TO COORDINATION/COOPERATION MODELING	29
5.1.1	DEFINITIONS	29
5.1.2	MODELING A CONFLICT FRAMEWORK WITH MULTIAGENT SYSTEMS	30
5.1.3	MULTI-AGENT REPRESENTATION FOR CRISIS MANAGEMENT AND INFORMATION IMPACT ANALYSIS	32
5.2	EXAMPLE OF MAS MODEL FOR INFORMATION IMPACTS IN COORDINATION	35
5.2.1	INDIVIDUAL AND SOCIAL RATIONALITY	35
5.2.2	MAS MODEL FOR COORDINATION UNDER VARIOUS INFORMATION SCENARIOS	36
5.2.3	CASE STUDY AND RESULTS	40
6.	CONCLUSION	46
7.	REFERENCES	47
8.	APPENDIX	50

1. FOREWORD

This report is intended to provide a conceptual framework for assessing the security risk to power systems assets and operations related to malicious attacks. The problem is analysed with reference to all the actors involved and the possible targets. The specific nature of the malicious attacks is discussed and representations in terms of strategic interaction are proposed. Models based on Game Theory and Multi Agent Systems techniques specifically developed for the representation of malicious attacks against power systems are presented and illustrated with reference to applications to small-scale test systems.

This report is the fruit of a cooperation between Politecnico di Torino – Dipartimento di Ingegneria Elettrica and the Joint Research Center of the European Commission – Institute for the Protection and the Security of the Citizen.

This document is organized as follows. In chapter 2, the problem of malicious attacks to critical infrastructures is described; chapter 3 analyzes the nature of malicious attacks and provides an evaluation of their potential cost and impact; the basic concepts of game theory and the examples for modeling the strategic interactions so as to assess the risk of malicious attack are introduced in chapter 4; multi-agent system model for studying coordination/cooperation and some applicative examples are provided in chapter 5; finally, conclusions are drawn in chapter 6.

2. INTRODUCTION

A vast number of hazards threatens public facilities both due to accidental reasons and intentional attacks; both of them may have disastrous social and economic effects. Deliberate attacks have always drawn particular concern; especially nowadays that international terrorism has become a very serious problem. Consequences of malicious attacks are usually serious, because they are intentionally performed for damaging a particular target. Some recent attacks provide terrifying examples: on September 11th 2001 four aircrafts crashed in the US and about 5000 people were killed, in Madrid 199 people were killed in train station bombing on 11th March 2004, while in London, suicide bombs killed 56 people and injured more than 700 others on 7th July 2005.

Among public facilities, the infrastructural systems for electric power delivery have a particular importance, since they are widely distributed and indispensable to modern society. Attacks against power systems may cause vast social and economic damage; hence power systems are a well known target for malicious attacks, also because they are constrained by specific physical laws that can be exploited to obtain the greatest effects from the attack.

Electrical systems are wide infrastructural systems that deliver the electricity generated by power plants to end-consumers. The main feature of power systems is their articulation in several networks operated at different voltage levels. They are usually divided in three subsystems: generation, transmission and distribution. Moreover, national power systems are usually connected with those of the neighbouring countries by high voltage tie-lines, thus establishing a continent-wide interconnected system.

The basic goal in operating power transmission systems is to transport electricity from the generation centers to the load centers in a reliable and secure manner. These systems must be operated within given thermal, voltage, and stability limits under a wide variety of conditions such as continuous variations in load, equipment unavailability and failure, wide range of weather and climatic conditions etc. .

Outages of power systems may have severe impacts on a country in many respects. The different events that may affect the electrical or physical integrity of a transmission system are due to various causes, which can be grouped in the following categories ^{[1][2]}:

- 1) natural causes such as lightning, storms, cold, ice, forest fires, and geomagnetic storms;
- 2) electro-mechanic, control and communication equipment failures, with either immediate or latent consequences that may only affect the system when the equipments are called into operation; this kind of failures can affect power system components, such as generators, transformers, and/or transmission lines; control and protection systems, such as hidden failures in protective relays, malfunctioning of circuit breakers, interacting controls, control failures, or misoperations; information and communication systems, such as loss of communication with energy management systems, inability to perform automatic control and protection functions, failures or congestion of the information systems, and intrusion of external agents into the information/communication systems;
- 3) human factor including human errors that are not intentional; examples are faulty settings of control and protection systems, system operator errors, manual control errors, and failure of operating personnel to follow the guidelines established for secure power system operation;
- 4) malicious threats, that are intentional attacks to the power system infrastructure; they can be physical or cyber attacks and can be simultaneous outages of power equipment (sabotage, bombing, etc...), simultaneous outages of communication equipment, and sabotage through communication system.

In the last decades the introduction of competition in the electricity industry depicted a completely new scenario in which the centralized decision making approach characterized by a vertically Integrated Industry has been replaced by the decentralized decision making process of a number of competing market players. In this new context the issues related with systems security, also against malicious players, propose new challenges and need to be revised.

2.1 GROWING CONCERN FOR THE SECURITY OF CRITICAL INFRASTRUCTURES

Malicious threats might target infrastructures such as power systems, water systems, public traffic systems, which are vital to the whole society and may cause very severe consequence once the failure happens. Different infrastructures may be considered as:

- *power systems*: there are some weak points in the power transmission system, e.g. the attack to some special nodes or lines will possible result in black out and cause big economy loss^{[3][4][5]};
- *hydro (water) networks*: hydro networks need to face the malicious destruction of the network and the attack with intentional toxicant drain in the water network, with the help of the modern science of chemistry and biology, the toxicant or pathogen may cause very serious problem to the people in terms of epidemic diseases^[6];
- *gas and oil networks*: the attack to the gas/oil network can influence the market price of the fuel, there will be the consequence on the economy and on the lack of energy resources, which will not be soon reflected by people daily life^[7];

- *informatics networks*: with informatics networks attacked, there will be the problem of communication and media, the out of control of the informatics networks will lead the society to panic^[3];
- *transportation networks*: as the subway systems have been attacked by the terrorists as in London and Madrid, the attack on transportation network is very quick to be known by the people and hugely influence the people's daily life, and the people suffer that directly, especially from psychology point of view^{[7][8]}.

All the systems listed above are critical to people's lives, because their failures are often disastrous for the whole society, in that they bring big economy losses and political and social problems altogether. Attacks to the transport systems seem to be the most practiced in recent times, especially against the public transport infrastructures like civil aircraft, railways and subways. However, malicious activities against other networks could cause very severe consequence as well. For example, the accidental blackouts of power systems that took place in the US and Italy pointed out the vulnerability of those systems and the huge impacts of such events (US blackout 9300 km² and 50 millions of inhabitants involved, 39 G\$/day of economic lost; Italian blackout 57 millions of inhabitants, 4 persons died, 120 M€ of economic loss).

In that respect, it may be recognized that other sources of raising concern like international criminal organisations may share with international terrorism some goals, e.g. blackmailing countries by menacing public security, as well as the most immediate targets, critical infrastructures that affect public life, and the concrete ways to perform attacks – bombs and cyber attacks for instance.

Hence, although the aims and the goals in those two international threats to public security are profoundly different, to all respect those differences will be rather immaterial in front of our purpose that is the modeling such threats and the specific attacks patterns is such a way as to be able to devise the most effective countenance and response strategies to such threats.

The impact of malicious attacks to critical infrastructure may be very serious for several reasons:

- the reliance on infrastructures of all societal and private functions;
- most probably attacks are explicitly designed to maximize damage and psychological impact on the public – as demonstrated by the Madrid and London cases;
- infrastructures are interconnected, and therefore cascading and escalating effects cannot be excluded.

A key concern relates to targeted attacks, e.g. against control and communication systems of critical infrastructures, or contemporarily against the physical infrastructure and its control system, as pointed out by the recent Communication of the Commission on Critical Infrastructure Protection in the fight against terrorism: *“The consequences of an attack on the industrial control systems of critical infrastructure could vary widely. It is commonly assumed that a successful cyber attack would cause few, if any, casualties, but might result in loss of vital infrastructure service. For example, a successful cyber-attack on the public telephone switching network might deprive customers of telephone service while technicians reset and repaired the switching network. An attack on a chemical or liquid natural gas facility's control systems might lead to more widespread loss of lives as well as significant physical damage.”*^[9]

The same communication points out how power systems might be the most specific target for such attacks, due to the synergistic effect with other infrastructures: *“Another type of catastrophic infrastructure failure might be when one part of the infrastructure leads to the failure of other parts, causing widespread cascade effect.*

Such failure might occur due to the synergistic effect of infrastructure industries on each other... Cascade events can be very damaging too, causing widespread utility outages. The blackouts in North-America and Europe during the last two years have put in evidence the vulnerability of energy infrastructures and consequently the need to find effective measures to prevent/or to mitigate the consequences derived from a major supply disruption.” ^[11] Although the main focus is on terrorism, other sources of malicious attacks are to be considered as both widespread and potentially very harmful, organised criminality in particular.

Power system failures cause severe consequence to regular daily life. The critical dependence of advanced economies upon electric power involves that power failures have wide socio-economic consequences, and provoke important psychological impact on the public. The blackouts and brownouts that happened in Europe and the United States in the last years showed that a vast number of hazards can threaten the system due to accidental reasons. In addition, they have revealed the potential vulnerability of the system to malicious attacks. Other than the direct economic losses, the New York City blackout of 1977 gives an example of how the blackout brought incredible social impacts to the people: *“Looting and vandalism were widespread, hitting thirty-one neighborhoods, including every poor neighborhood in the city. In all, 1,616 stores were damaged in looting and rioting. 1,037 fires were responded to, including 14 multiple-alarm fires. In the largest mass arrest in city history, 3,776 people were arrested. Many had to be stuffed into overcrowded cells, precinct basements and other makeshift holding pens. A Congressional study estimated that the cost of damages amounted to a little over US\$300 million.”* ^[9] Moreover, in recent years, the blackout or the disruption of the power system are frequently take places in the world, for instance, in the summer of 2003, the blackout/disruption concentrated within 6 weeks and hugely affected the lives of 112 million people in 5 countries ^[10]:

- 1) August 14, 2003- North East blackout over the US and Canada
- 2) August 28, 2003 - Southern London distribution
- 3) September 23, 2003 - Danish/Swedish blackout
- 4) September 28, 2003 - Italian transport grid collapses.

Despite the cause of the problem, and due to the increasing interconnectivity of the grid, a failure of the electric power infrastructure may have disastrous effects over a broad geographic area, even crossing national borders.

2.2 CLASSIFICATION OF THREATS TO INFRASTRUCTURES

There is no generally accepted definition of threat. From the legal point of view, a threat by an agent consists of the unwanted (deliberate or accidental) expression of intent to execute action that may result in harm to an asset. Therefore, a threat is the potential occurrence of a negative action, not its actual realization. In the case of critical infrastructures, the consequence of an attack can be much more serious that originally intended.

Threats to infrastructures can be broadly classified into two main categories: *physical* and *cyber threats*. The first category includes any action aimed to destroy some physical components of the network. For power systems, targets may be, power stations, transmission lines, transformation sub-stations. The second category includes deliberate actions to cause failure in the communication systems that are used to monitor and control the systems; for instance, communication links over power lines and other telecom channels to carry tele-metering signals, power system control software etc.. Tab.2.1 reports three different types of physical threats., while Tab.2.2 provides a list of cyber agents that might jeopardise critical infrastructures.

Table 2.1 - Physical threats to Critical Infrastructures

Threat	Description
Natural Hazards	Natural disasters have accounted for a large percentage of the malfunction of the infrastructure, Geomagnetic storms, earthquakes, forest fires and tsunamis all represent significant natural hazard threats to the critical infrastructure.
Accidental threats	Accidents are, by definition, unforeseen, and therefore, difficult to predict.
Malicious threats	<p>Infrastructures have long been targets for malicious attack, whether for criminal military or political purposes. There are a range of actors, employing a range of tools (from conventional weapons, weapons of mass destruction- including chemical, biological radiological and nuclear agents) who have displayed a willingness to engage in malicious activity direct to physical critical infrastructure. Four major objectives in describing an aggressor's behavior are:</p> <ul style="list-style-type: none"> • destroying or damaging critical facilities, property, or equipment • stealing or damaging critical equipment, materials • posing a threat to the safety of personnel or customers • creating adverse publicity.

Table 2.2 - Cyber threats to Critical Infrastructures

Threat	Description
Crackers, Malicious hackers, Script-kiddies	All these figures refer to individuals with certain knowledge of computer and communication systems, which break into systems violating security measures. They sometimes crack into networks for the thrill of the challenge or for bragging rights in their community. While remote cracking once required a fair amount of skill or computer knowledge, one can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Insider threat	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions, because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data.
Malware writers	Malicious code writers produce software designed specifically to damage or disrupt systems, such as a virus, a worm or a Trojan horse. These are normally known as malware. They can be specific (target to particular systems or even organisations), or generic.
Criminal groups, organised crime	There is an increased use of cyber intrusions by criminal groups who attack systems, mainly for monetary gain. These groups might try to get internal information for blackmailing the company, or to extort by menacing the dissemination of some sensible information, or to commit different types of fraud (e.g. influencing some prices), or forgery (e.g. changing values in bills).

Hacktivists	<p>Hactivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.</p> <p>Their activity against infrastructures can be motivated by environmental, safety, or nationalistic reasons – but this is hardly related to the targeted systems. The objective of a certain action could be to stop a certain infrastructure from carrying out their normal operations.</p>
Terrorist groups	<p>Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.</p> <p>Terrorism has targeted infrastructures, but mainly from the physical viewpoint. Few cyber-actions have been registered. Attacking infrastructures could be an effective way to jeopardise governments, or intimidate the citizens of a country.</p>
Information warfare	<p>Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that can affect infrastructures as one key column of a country.</p>

Source: [12]

2.3 ACTORS IN CRITICAL INFRASTRUCTURES

Different actors are involved in the context in which terrorist threats and attacks are implemented. Malicious attackers wish to implement attacks to infrastructures in such a way as to maximize the impact on the public and stakeholders, while government, authorities and stakeholders act in such a way as to minimize risks and effects of the attacks. We can define the three main actors as:

- Attacker:* the individual or organization aimed to provide damages to the infrastructures; malicious attackers may include experts with professional knowledge about the power system, able to assess the impacts of the attack to a specific target;
- Defender:* all the forces committed, at various levels, to protect the potential targets, such as government, police, power system operator (SO);
- Sufferer:* common people that will suffer of the attacks and may put pressure for fear on the government to change his policy.

Fig.2.1 shows the basic interaction among the above actors referred to malicious attacks.

Potential attackers may retaliate the defender organisations by threatening to implement attacks once their demand is declined by the defender organisations. Defender organisations, namely the government, may compromise with the terrorists under pressure from the public opinion. This is a complex interaction, which should be carefully studied. Networked infrastructures such as power systems, transportation networks, water supply networks etc. are widely distributed systems, so that the effects of localized attacks are amplified: the attack to just one component of the system can provoke a major failure of all the system due to its structure and to the physical and operational constraints that need to be met.

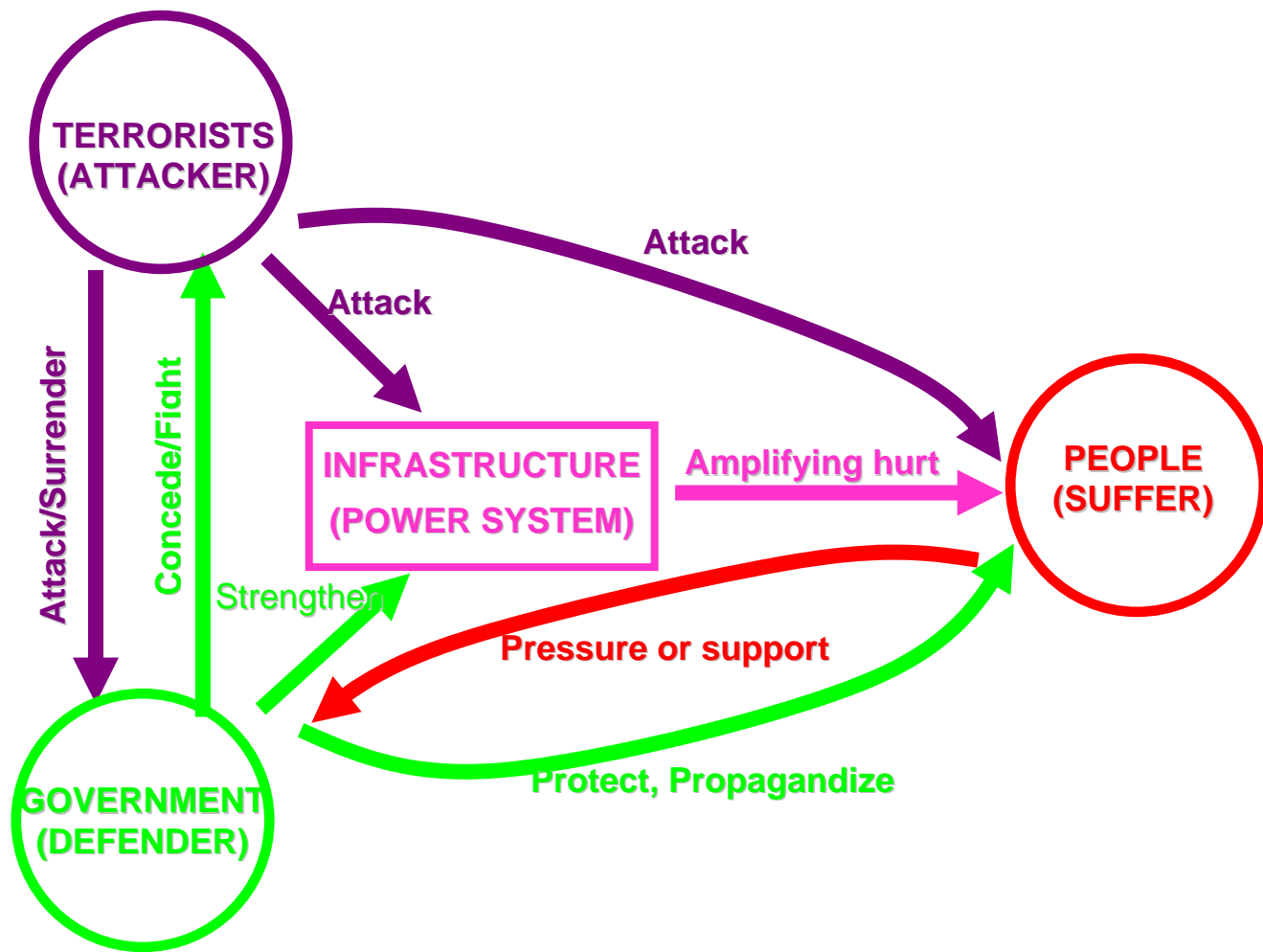


Fig. 2.1 - Interaction scheme among the players in malicious attacks

3. MALICIOUS ATTACKS AND DEFENCE STRATEGIES

A malicious attack is a set of actions that specifically aim to do harm upon a target system. They are premeditated, with a motivation that can be political (e.g. terrorism), illegal (e.g. organized crime) or just malevolent (e.g. hackers) and executed by threat agents who may be totally external to the system or have internal access to and/or knowledge of it.

In the case of critical infrastructures, the consequence of an attack can be much more serious than originally intended.

3.1 NATURAL VERSUS MALICIOUS THREATS

By threat we mean potential adversarial events. When we study the security of the infrastructure, for instance power systems, there are two types of security control. One is the preventive control and the other is the corrective control. The former one is to take countermeasures before the happening contingency while the latter is performed after the contingency. From this point of view, threats are to be analysed in view of discovering vulnerabilities of preventive controls.

Natural threats

Natural threats are potential adversarial events that occur without the man's intentional intervention. Such threats are due to inner component failures during system operation due to aging etc., unintentional mis-operation of the system, and other natural phenomena such as atmospheric discharges (lightning), animals, winds etc. which may impact on the operation of the infrastructure. All these failures are the subject of statistic studies, based on which the research branch of reliability was developed.

Malicious threats

Malicious threats imply a willingness to make damage, which is a critical topic to the security of the infrastructures. In that respect, some features of the malicious threats are to be emphasized:

- malicious threats are selective, the more the target may produce disruptive effects the more it is likely to be attacked;
- malicious threats are selective, as more as the target is protected as less will be likely to be attacked;
- the level of threat, for a given component, depends on the attitudes, decisions and interaction between attackers and defenders at a given point in time and space;
- malicious threats are always referred to criminal or illegal activity

Comparison between natural and malicious threats

There are huge distinctions in various aspects between malicious versus natural threats. The conventional methods for dealing with natural threats are not applicable to malicious ones. In malicious threats, strategic interaction among players determines the probability and the real occurrence of an attack in time and space, while natural based threats to power system occur on random base (nature has no specific willingness to hurt, nature is a "random" player). In other words, a malicious threat modifies the probability distribution of the contingency, so that the contingency corresponding to more severe consequences and easier attack implementation will be

assigned extra probability of occurrence due to the consideration of malicious threats. Tab. 3.1 introduces a side by side comparison of the two threats.

Tab.3.1 - Comparison between the natural and malicious threats

	NATURAL THREATS	MALICIOUS THREATS
MOTIVATION	accidental	rationally deliberately
DISTRIBUTION ON THE SYSTEM	random	critical component preferred
RISK ASSESSMENT	probabilistic approaches (Monte Carlo simulation)	rational interactions models
COUNTERACTIONS	re-enforce the system	1. re-enforce the system 2. preemptive measures against terrorists
STRATEGIC INTERACTION	No	yes
PLAYERS	1. SOs 2. sufferers	1.SOs 2.terrorist organizations 3. government 4. sufferers

3.2 IMPACT OF ATTACKS AND DEFENCE/ATTACK COST

Europe counts for many infrastructural systems that for their importance for national security and societal welfare are critical, and should be protected accordingly. Due to their geographical extension and to technological evolution it is difficult to determine the more appropriate level of protection. Moreover, pervasive application of information and communication technologies (ICT), and market liberalisation introduce many new opportunities for malicious threats, and the consequent happening and cascading of dangerous events.

The understanding of the infrastructural risks caused by deliberate man-made actions should be done in the context of a systematic Security Framework. Once the problem is framed, it would be possible to conduct a Security Assessment, i.e. a risk-oriented analysis of the system for the analysis of the assets that could be menaced by internal and external threats.

However, a crucial issue in this process is how to profile the behavior of a malicious intruder in the system, in such a way as to select the most appropriate defensive pattern, while the attack develops – taking into account that the intruder also learns from the defender while this deploys his defense.

In the following, we focus on power transmission grids. The subsystems and components to be considered are:

- *Transmission lines*: composed of towers, cables/wires and insulators.
- *Substations*: composed of building, control and communication systems, transformer and breaker.
- *Control Centre*: composed of building, operators, control and communication systems

A critical issue for analyzing the scenarios related to malicious attacks is referred to the assessment of the impacts that malicious action against power system can provide.

Different types of impacts need to be considered. The usual way to assess the impacts of a failure in power system is related to the amount of unserved energy. An average economic value of unserved energy can be computed as the Gross Domestic Product (GDP) divided by the energy consumed per annum. Taking the case of Italy, we have:

$$u_e = \frac{1465594.4 \times 10^6}{330 \times 10^9} = 4.44 \text{ €/Wh}$$

Of course the value of the unserved energy can be weighted somehow on the location in which the energy is not provided since it may be more important, for example, a big town than the countryside. A different method to evaluate the economic impact of electrical energy interruptions is through direct assessment of customers. Starting from the consideration that customers are themselves the most able in characterizing the impact of interruptions, this method is based on surveys of the subjective costs or losses that the customers suffer for different kind of interruptions (time of occurrence and duration). Even if significant efforts, in terms of number of customers involved and time, are needed to obtain meaningful results, the direct assessment is currently the most appreciated method.

In addition to the economic impact, other impacts should be considered such as those related to psychological and social disorders, and given an equivalent economic value to make them comparable and additive in the analysis.

The possible defense actions can be classified in on-line and off-line interventions. For the offline intervention, some devices and the related costs are reported in Tab.3.2..

Tab.3.2 - Defense actions and corresponding cost per subsystem and component

MEASURE	DESCRIPTION	COSTS
Control and Protection systems	These devices either react automatically to faults or report to operators the grid state for further action.	- Load shedding relays: 3000 € per apparatus, 1000 installed in Italy. Hence to duplicate their number would cost 3 € Mio; -The Critical sections (with foreign countries), 20 apparatus, cost 50 k€ per apparatus + 500-600 k€ for the central SCADA, called Energy Management System (EMS).
Power electronic devices	Series compensation, phase shifters. These devices change the impedance of one line	The cost can be estimated at about 50 € per kW
Interruptible loads	large consumers accept a contract type that allows the provider to interrupt electricity delivery	Their equivalent cost is some 300 € Mio per annum in Italy
New transport lines	Can be built to strengthen the grid	Some .2-.3 € Mio per km in Italy
Cybersecurity measures	e.g. improved firewall, access control and intrusion detection systems	- 20 K € per substation - 100 K € per Control centre
Physical protection	including the hardening of buildings, fencing, protecting walls, etc.	.5 – 2 € Mio per target

Attackers need to put some human resources and physical – and cyber - resources (e.g. explosives, delivery tools etc) in targeting a system component. While the cost of the former is of course difficult to quantify the latter is more predictable; anyway, both those monetary and non monetary aspects of an attack need to be quantified in monetary units; they depend on the components, their location, their

protection level etc.. A gross economic evaluation of the cost of physical resources to perform attacks per component is given in Tab.3.3.

Table 3.3 - Attacks and corresponding cost per subsystem and component

Subsystems	Components	Attacks	Measure	Cost (K€)
Lines	Poles	Physical	Bomb	50
	Cables/Wires	Physical	Short-circuit	10
	Insulators	Physical	Projectile	10
Substations	Building	Physical	Bomb	100
	Control & Communication system	Cyber	DOS	50
		Cyber	Intrusion	100
		Physical	Cut/Destruction	500
	Transformers	Physical	Bomb	1000
	Breakers	Physical	Bomb	100
Control centre		Physical	Short-circuit	50
	Building	Physical	Bomb	1000
	Operators	Physical	Incapacitation	100
	Control & Communication system	Cyber	DOS	100
		Cyber	Intrusion	500
		Physical	Cut/Destruction	1000

4. MODELLING OF THE STRATEGIC INTERACTIONS IN MALICIOUS ATTACKS

In summary, malicious attacks are carried out by intentional attackers, who are rational in terms of maximizing the impacts they can get from their actions, choosing the most influential targets. Power systems are characterized by severe physical and operational constraints that need to be met to keep their operation feasible; those constraints may be known by attackers skilled and trained enough to take advantage so as to maximize the effects of their attacks by exploiting the amplifying effects that those constraints imply. The possibility to implement successfully those attacks and their actual outcome depend on the counter measures undertaken by the defenders - the government and their police and defense forces, stakeholders etc.. Defense actions may discourage the attackers and prevent possible attacks to given targets; the decisions of each part influences the decision of the other, so that this problem may be classified, as a *strategic* problem where complex interactions take place among the players^[13]. Proper models are needed to represent such a context and the outcomes of those studies are useful to predict the behavior of the terrorists and help the authority to design proper defense plans and actions.

4.1 GAME THEORY APPLICATIONS TO MALICIOUS ATTACKS MODELING

Game theory was originally devised to model conflict situations and was successfully applied for modeling the interplay among different actors in several fields e.g. information technology^[15], transportation industry^[16], stock market^[17], electricity market^{[18][19]} and sociology^{[20][21]}. More broadly, game theory proved to be a useful tool to model complex relations inside economic, political, cultural problems wherever it is needed to model human activities in a strategic scenario, where the factors involved may range from political to economical, religious, national, technologic, historic, cultural issues.

4.1.1 DEFINITIONS

Game theory is devoted to the formal study of conflict and cooperation. Game theory concepts apply whenever the actions of several entities (players) are interdependent in the sense that the utility got by a player in the games depends on the move of others players. These agents may be individuals, groups, firms, or any combination of these. The concepts of game theory provide a language to formulate, analyze, and understand strategic scenarios.

Game theory was introduced in 1944 by Von Neumann and Morgenstern^[22]. In 1950, John Nash proved that Nash equilibria must exist for all finite games with any number of players^[23]. In the last 50 years, game theory becomes a crucial tool for the analysis of strategic behavior of individuals and particularly for studying competition among the companies in an oligopoly markets.

Game theory is concerned with the actions of decision makers who are conscious that the actions of their competitors affect their utility.

The essential elements of a game are *players*, *actions*, *payoffs*, and *information*. These are collectively known as the rules of the game, and the modeler's objective is to describe a given scenario in terms of the *rules of a game* so as to model the context and figure out what will happen in that scenario.

The hypothesis of the rational player, according to which each player will act so as to maximize a measure of his/her own utility, is assumed.

The basic elements of a game are defined as follows:

- Players: individuals/entities that make decisions
- Action set: choices available for each player
- Payoff: utility that each player receives at the end of the game
- Strategy: a rule that tells a player which action to take at each instant of the game, given his information set.
- Game order: order of moves in non simultaneous game.
- Information set: knowledge available to each player when he/she decides the action
- Nature: a non-player who takes random actions at specified points in the game with specified probabilities

Two different types of strategies can be considered in the game:

- Pure strategy: each player chooses with unit probability only one move in the action set;
- Mixed strategy: each player individuates a probability distribution over the action set; to each move corresponds a probability and the probabilities of all moves sum up to one.

and the payoff structures can be set with reference to two possible alternative schemes:

- Zero sum games: the measure of the total utility to all the players in the game, for every combination of strategies, always adds to zero. One wins exactly the amount one's opponents lose.
- Non-zero sum games: a gain by one player does not necessarily correspond with an equivalent loss by another.

Other features of the games are:

- Cooperative/non-cooperative game: players are able/unable to make enforceable agreements.
- Symmetric/asymmetric game: a symmetric game is a game where the payoffs for playing a particular strategy depend only on the other strategies employed, not on who is playing them. Otherwise, it is an asymmetric game.
- Static (simultaneous) game: in *static game*, all players make decisions simultaneously, without the knowledge of the strategies that are being chosen by other players, or if they do not move simultaneously, the later players are unaware of the earlier players' actions (making them effectively simultaneous).
- Dynamic (Sequential) game: a game where one player chooses his action before the others choose theirs and the later players must have some information of the choice of the previous players.

The most important aspect in a game is the possibility to find an *equilibrium*. Therefore the equilibrium represents the searched outcome of the game; it is determined by the intersection of the strategies actually chosen during the game by all players.

Information context

In game theory, an information set indicates what a player knows when it is his/her turn. With respect to the information of the game, several conceptions are defined:

- *perfect/imperfect information*: perfect information means that in the game, each player knows every action of the players that moved before him/her at every point, while the imperfect information is defined as games where a player does not know exactly what actions other players took up to that point.
- *complete/incomplete information*: in the game with complete information, knowledge about other players is available to all players. Every player knows the payoffs and strategies available to other players. Otherwise it is a game with incomplete information.
- *symmetric/asymmetric information*: in the game with symmetric information, no player has information different from those of other players while asymmetric information means that there exists difference in the information the players have.
- *certain/uncertain information*: certain information is used to describe a game in which all players know exactly what game they are playing in the sense that they know what the payoff of playing a particular strategy will be given the strategies played by other players. Particularly in the context of extensive form games, a game of certain information is to be defined as any game in which nature does not move after the players have moved.

Equilibrium types

- *Strong/weak dominant strategy equilibrium*

A strategy S_i^* is said to be a *dominant strategy* if the player, with its choice, gets his/her maximum payoff, for whichever move of his/her counter parts, in formula:

$$\pi_i(S_i^*, S_{-i}) > \pi_i(S_i', S_{-i}) \quad \forall S_{-i} \quad \forall S_i' \neq S_i^*$$

where:

π_i is the payoff of the i -th player

S_{-i} is the strategies of the i -th counterparts.

A weak dominant strategy differs from a strong one only for the weak inequality:

$$\pi_i(S_i^*, S_{-i}) \geq \pi_i(S_i', S_{-i}) \quad \forall S_{-i}, \quad \forall S_i' \neq S_i^*$$

Equilibrium with a strong/weak dominant strategy is represented by a combination of moves that are strong/weak dominant strategies of the players.

- *Nash equilibrium*

A Nash equilibrium is a set of strategies, one for each player, such that no player has incentive to unilaterally change his/her action. Players are in equilibrium if a change in strategies by any one of them would lead that player to earn less than if he/she keeps the current strategy.

The strategy profile S^* is a Nash equilibrium if no player is motivated to change their move if the others do not. In formula:

$$\forall i \quad \pi_i(S_i^*, S_{-i}^*) > \pi_i(S_i', S_{-i}^*) \quad \forall S_i' \neq S_i^*$$

where:

S_{-i}^* is the strategy of i 's counterparts at equilibrium.

A Nash equilibrium is optimal according to Pareto.

- *Pure strategy equilibrium/mixed strategy equilibrium*

pure strategy equilibrium, in which each player chooses one and only one move in the action set;

mixed strategy equilibrium, in which a strategy consisting of possible moves which corresponds to the probability distribution (collection of probabilities, can be a measure of the possibility of taking the corresponding action).

Existence/uniqueness of equilibrium

In a game, generally speaking, it is not sure that an equilibrium exists or that it is unique. Some particular criterions are drawn as:

- in a game with a finite number of actions, Nash equilibrium always exists, at least, with mixed strategies;
- if an equilibrium with dominant strategy does exist then it is unique.

4.1.2 THE SEARCH FOR AN EQUILIBRIUM

Every participant in the game would like to maximize its utility, which is influenced by the decision of the other players. With all the factors that may impact the payoff of the players taken into account, the approaches for finding the equilibrium can be concluded as follows:

- A simultaneous game can be given a matrix representation in a *Strategic (or normal) form*. For two players, one is the "row" player, and the other, the "column" player. Each row or column represents a move and each box represents the payoffs to each player for every combination of strategies moves. Generally, such games are solved using the concept of a Nash equilibrium ^{[22][25]}. In the case of three players, as illustrated by Fig.4.1, the normal form can be displayed as a three dimension matrix with strategies $(a_1, a_2 \dots)$ for player A , $(b_1, b_2 \dots)$ for player B , $(c_1, c_2 \dots)$ for player C and corresponding payoffs as entries.

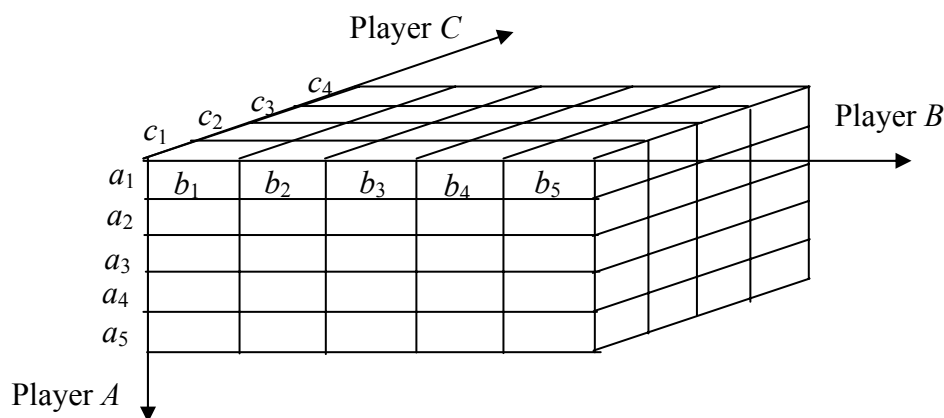


Fig.4.1 - Three dimension normal form representation of the game

- *Deletion of dominated strategies* as a way to approach the equilibrium; it is one common technique for solving games and is based on iteratively removing

dominated strategies. In the first step, all dominated strategies of the game are removed, since rational players will not play them. This results in a new, smaller game. Some strategies -- that were not dominated before -- may be dominated in the smaller game. These are removed, creating a new even smaller game, and so on.

- *Intersection of the best response functions*, the best response is the strategy (or strategies), which produces the most favorable immediate outcome for the current player, taking other players' strategies as given. The concept of a best response is central to the Nash equilibrium which is dependent on each player selecting the best response. From another point of view, we can find Nash equilibrium of a game in which each player has only a few actions by examining each action profile in turn to see if it satisfies the conditions for equilibrium. In more complicated games, it is often better to work with the players' 'best response functions'.
- *Backward induction* is an iterative process for solving finite extensive form or sequential games. First, one determines the optimal strategy of the player who makes the last move of the game. Then, the optimal action of the next-to-last moving player is determined taking the last player's action as given. The process continues in this way backwards in time until all players' actions have been determined. Eventually one determines the *Nash equilibrium* of each subgame of the original game ^[26].
- *Uniform expected payoff of the nonzero probability actions* for the mixed strategy equilibrium. It is a useful approach derived from the characterization of mixed strategy Nash equilibrium, in which the probability assignment to the defender's/attacker's actions should make uniform the utilities of the attacker's/defender's nonzero probability actions. Moreover, the utility of the nonzero probability actions should be greater than that of the zero probability actions.

4.1.3 APPLICATION OF GAME THEORY TO STRATEGIC INTERACTION IN MALICIOUS ATTACKS TO POWER SYSTEMS

As discussed in the introduction to this chapter, a strategic interaction takes place in malicious attacks, which is suitable to be described by game theory. The game theory application is confined by some rational hypothesis, which may not be true in reality due to the limitation of the players' capability and the information set they have.

Sandler, Tschirhart, and Cauley^[27] present some rational-actor models that depict the negotiation process between terrorists and government policy makers for incidents where hostages or property are seized and demands are issued. In this model, terrorists' valuation of the likely concession to be granted by a government is based on a probability distribution conditioned on past government concessions. Their analysis illustrates that the terrorists' choice and actions are influenced by those of the government and vice versa.

Especially after the disaster of Sept. 11, 2001, many research efforts investigated application of game theory to threats to critical infrastructures. Sandler and Arce^[28] listed six strengths of modern game theory for revealing quantifiable factors theoretically underlying the behavior of terrorists and targeted governments:

- *captures the strategic interactions between the game players, namely the terrorists, the government, the common people, that can make decisions independently; there are direct conflicts among those players, hence whatever decision made by one player will surely influence the behavior of the others;*

- *helps discover the strategic implications when each side acts according to its best guess about how the other side thinks;*
- *incorporates the impact of threats and promises from each side;*
- *takes advantage of the observation that players tend to maximize goals subject to constraints, and every one involved in the conflict has its own definite objective;*
- *helps predicting outcomes in bargaining over demands;*
- *acknowledges the impact of uncertainty—incomplete information—on all the above.*

Basically, existing researches on modeling with game theory defense strategies against malicious attacks are focused on the following topics:

- how the government may choose strategy with respect to non-negotiation or concession. More specifically, for the kidnap and hijack ^{[29][30]}.
- how attackers choose the target country, i.e. with the best payoff expectation, so that expected pay-off in one country affects estimated pay-offs in other countries ^[31].
- how the government chooses the strategy with respect to deterrence or pre-emption^{[32][33]}. E.g. Daniel and Arce ^[34] analyse the effect of those two strategies taking interaction between US and Europe in that respect as the playfield. A different choice of strategy by one player will influence not only its own benefit but also that of the other players. Hence coordination is necessary to coordinate to get the best overall strategy.

In general these approaches are focused on strategic choices, namely who will be the target, deterrence vs. preemption, negotiation vs. concession, how to bargain with terrorists etc. without special consideration for the physical conditions the attack shall take place into. As mentioned in 2.1, the existent literature on game theory application to terrorist attacks to critical infrastructures lacks in domain specific analysis taking into account their peculiar physical features. A model based on mixed strategy equilibrium was developed in [4], in which, the power system components are ranked with the probabilities of being attacked and defended in terms of the probabilities of the attack and defense actions. The payoff sensitivity analysis with reference to the defense action and the resource of the both attacker and defender sides are performed. Results show an obvious amplifying effect of the power system for the malicious attack.

4.2 EXAMPLE OF GAME MODEL FOR RISK ANALYSIS IN MALICIOUS ATTACKS

In this section, considering the specific features of the power system, we develop a game model to represent the interaction between the terrorist and the SO when attacking/defending the network.

The goal of the attacker is to maximize the impacts of its attacks: this may be roughly measured by the loss of load, in terms of the power in MW that cannot anymore be supplied after the attack. The power at different buses of the network can be associated to different loads at different locations in the grid. This loss of load measures, at the same time, the negative outcome to the defender and the gain for the attacker - in this sense the “utilities” that defender and attacker take in the context are conflicting.

This model provides the equilibrium between attacker and defender, in terms of the set of discrete probabilities for their attacking and defending actions.

Different attack actions will target specific power system components (power lines, substations, ...). Each action has an associated cost to be undertaken, both for the attacker and the defender (Tab. 3.2 and 3.3) and a probability of success.

The probability of an attack to be successfully implemented (the probability of an attack times the probability of success) along with the damages associated to each of them provides the risk associated to a possible equilibrium in the interaction among the players and allows for a ranking of the system components in terms both of their likelihood to be attacked and of the associated risk. That represents the basic for designing proper defense plans.

A sensitivity analysis can be undertaken in terms of the changes in the equilibria and so of the attack patterns for variations in different aspects as the constraints in the resources allocated from the attacker and the defender to their actions or to the implementation of the defense action devisable. This kind of analysis can provide useful information for devising proper defence strategies.

4.2.1 MODEL DESCRIPTION

Due to the fact that the defender and the sufferers share in long term the same interest, they both don't like the terrorist and their goal is to protect the people (sufferers) from hurt, the only difference is that the defender owns the forces hence more tough, while the sufferers have the right to votes and are more willing to compromise with the terrorists when they are attacked. To simplify the game, the interaction between the sufferer and the defender is omitted and the sufferer is taken as a part of the defender. Due to the fact that the utility of the defender and the attacker is completely conflicting, the interaction can be modeled as a zero sum game, in which, the loss of one side is the gain of the other side.

The system vulnerability and the associated risk analysis can be carried out in terms of the equilibrium of the game between the defender and attacker. With the variation of the system configuration (new line, new bus construction, strengthen of the power system components which can be represented by lowering the destroy rate), the resources of the defender and the attacker, the equilibrium is accordingly changed hence the risk assessment should be performed along with the time. It should be noted that defending actions may require long time for their deployment, whereas the attacking patterns require less time. For example, the construction of a new line to reinforce the system may require from some months to years; instead, a terrorist group may suddenly change its attack target.

The equilibrium is related to a given scenario, characterized by a certain system configuration, attack and defend costs and budget limitation of the palyers; if the configuration changes, either because defense measures or attack patterns change, a new equilibrium must be found and a new risk analysis has to be carried out. In the Fig. 4.2, the temporal representation of the game is depicted, showing that for each variation, a new game is established with a new equilibrium. For example, between two time points t_1 and t_2 , a defense action has been implemented with a possible variation in the attacking patterns.

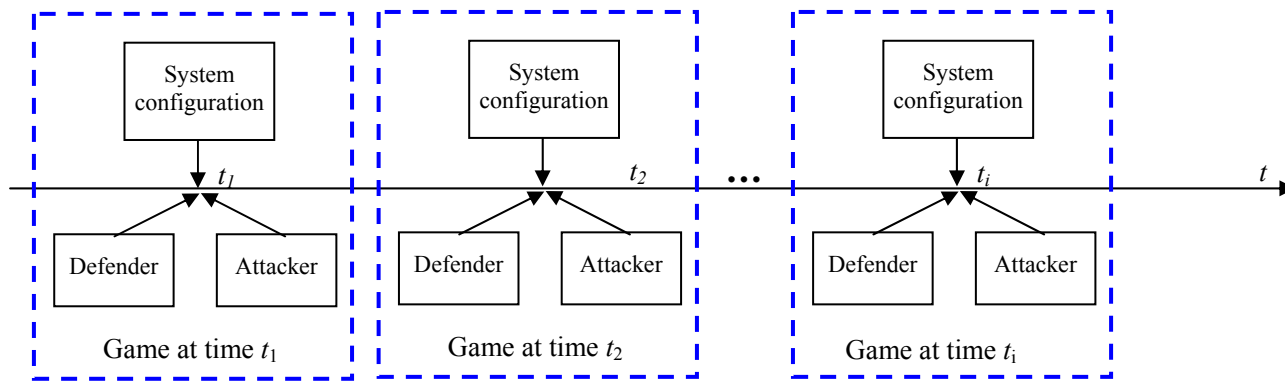


Fig. 4.2 - Risk analysis based on game model along the time axis.

Defender and attacker actions and resources constraints

We consider as possible targets some of the main components of the power systems as the transmission lines and the substations. Defense and attack actions against/in favor of multiple targets can be conceived and implemented. We define the set of desired simultaneous attack actions as:

$$\mathcal{T} = \{ a_1^t \dots a_k^t, \dots a_m^t \} \quad (4.1)$$

and the set of simultaneous defense actions as:

$$\mathcal{F} = \{ a_1^f, \dots a_k^f, \dots a_n^f \} \quad (4.2)$$

The number of actions that both the attacker and the defender can implement depends on their costs and is constrained by the resources they have available. Although these resources may include non monetary items, they may be reduced to an equivalent budget B_A , for the attacker and B_D , for the defender. The total costs of all the actions undertaken by each player need not to exceed the available budget. In formulas:

$$C_k^A = \sum_{i \in a_k^t} C_i^a \leq B_A \quad (4.3)$$

$$C_k^D = \sum_{i \in a_k^f} C_i^d \leq B_D \quad (4.4)$$

where:

- C_k^A cost of the attacker for implementing the attack action a_k^t
- C_k^D cost of the defender for implementing the defense action a_k^f
- C_i^a cost of attacking the component i
- C_i^d cost of defending the component i

Payoff of the players

The payoff of the attacker S_A is:

$$S_A = C_D + L_D - C_A \quad (4.5)$$

while the payoff of the defender is:

$$S_D = C_A - C_D - L_D \quad (4.6)$$

where C_A is cost of the attacker to perform an attack action C_D is the cost of the defender to perform a defence action, L_D is the economic value of a loss of load in the system and can be expressed as:

$$L = \sum_{j=1}^n \gamma_j \Delta D_j \quad (4.7)$$

where γ_j is the equivalent economic value of the load at bus j that is reduced due to the attack of the amount ΔD_j and n is the number of buses in the network. The load at different buses may have different importance from the strategic and economic point of view and the γ_j coefficient can account for that.

Crisis management

Under attack, after one or more components have been destroyed, the system may be not feasible and the SO needs to shed loads and change the set-points of the generators in order to restore the normal operating condition for the system. The transient process is not considered and the related dynamic stability problem disregarded and the generators are assumed able to smoothly reduce their power output according to the load shedding, i.e. the unbalance of the power supply and consumption caused by the lost of lines can be safely removed by generator output reduction.

We represent the strategy adopted by the SO as a constraint optimization problem in which the objective is to minimize the equivalent economic value of the loss of load D , the equality constraints are the DC power flow equations and the inequality constraints are related to the line flow limits and generators' production limits. In formulas:

$$\min L = \sum_{j=1}^n \gamma_j \Delta D_j \quad (4.8)$$

s.t.

$$\mathbf{B}\underline{\theta} = \underline{P} \quad (4.9)$$

$$|f_l| \leq F_l^{max} \quad l=1,2, \dots, n_l \quad (4.10)$$

$$0 \leq \Delta D_j \leq D_j \quad j=1,2,\dots, n \quad (4.11)$$

$$0 \leq g_j + \Delta g_j \leq G_{jmax} \quad j=1,2, \dots, n \quad (4.12)$$

where:

\mathbf{B} nodal admittance matrix, $\dim(\mathbf{B}) = nxn$

$\underline{\theta}$ vector of bus angle, $\dim(\underline{\theta})=n$

\underline{P} vector of bus power injection, $\dim(\underline{P})=n$

ΔD_j demand variation at bus j

D_j demand at bus j , before the attack

g_j original generated power at the bus j

Δg_j original generated power and the generation variation at the node j

g_{jmax} original generated power and the generation variation at the node j ,.

f_l line flow in line l

F_l^{max} line flow limit of the line l

n_l number of lines in the network

Equilibrium search

The payoff of the defender and attacker with reference to k -th scenario (defender takes the action i , and attacker takes the action j):

- Attacker :

$$S_A^k = C_D^i - C_A^j + L_D^k \quad (4.13)$$

- Defender:

$$S_D^k = C_A^j - C_D^i - L_D^k \quad (4.14)$$

where:

S_A^k : payoff of the attack in the k -th scenario;

S_D^k : payoff of the defender in the k -th scenario;

C_A^j : cost expressed in monetary value of the attacker for implementing attack action j ;

C_D^i : cost expressed in monetary value to the defender for implementing defense action i ;

L_D^k : loss caused by the power system failure in the k -th scenario, i.e. the effect of the attack/defense action.

With the payoffs of the defender and attacker in each scenario computed, the game can be solved with a one shot optimization approach based on the mixed strategy equilibrium characterization of the uniform expected payoff of the nonzero probability actions. The probability assignment to the defender's/attacker's actions should make uniform the utilities of the attacker's/defender's nonzero probability actions; moreover, the utility of the nonzero probability actions should be greater than that of the zero probability actions. A set of equations with respect to the '*uniform utility*' can be built and the equilibria can be derived. Considering different cases of the zero probabilities assignment to the actions, there would be an explosive of the case number to be analyzed hence hard to be calculated.

To solve the problem we transform the discrete cases analysis to a continuous optimization problem, which avoid the numerous case studies and conveniently find the mixed strategy equilibrium with the optimization algorithm.

Vulnerability ranking of the components

At the equilibrium we get a set of probabilities related to each possible action of the attacker and the defender. For the i -th component O_i , the attacking probability is:

$$P_i^a = \sum_{\forall O_i \in a_k^i} p_k^A \quad (4.15)$$

where $a_k^i (O_1, \dots, O_i, \dots, O_n)$ is the k -th action assigned with the probability p_k^A .

Once a component i is attacked it can be or cannot be destroyed both in the case that it is defended by the defender with some proper actions or not; of course the probabilities of disruption are different in the two cases. We define the successful destroy probability vector of the attack without the corresponding defense action taken:

$$\underline{\alpha} = \{ \alpha_1, \alpha_2, \dots, \alpha_{nc} \} \quad (4.16)$$

while with the defense action taken, the successful destroy probability vector of the attack is

$$\underline{\beta} = \{ \beta_1, \beta_2, \dots, \beta_{nc} \} \quad (4.17)$$

where nc is the number of the system component that can be attacked.

4.2.2 CASE STUDY AND RESULTS

We apply, for illustrative purposes, the model introduced in the previous section to a 30-bus system to analyze the system security in terms of the interaction between the attacker and defender in following aspects:

- evaluate the equilibrium with reference to the action of the defender and attacker and discover the system vulnerability by the components ranking;
- analyze the payoff sensitivity to the defense actions, base on which, the reference defense plan is designed;
- analyze the payoff sensitivity to the resource of the defender and attacker, to find out how the different resource allocations impact threats from malicious attacks.

Sample system

The sample IEEE 30-bus system consists 41 branches, 20 loads and 6 generators system as shown in Fig.4.3. Line data, generation and load data are respectively given as Tab. 4.1 and Tab.4.2, The data related to the attack/defense actions and probability of successful attack are reported in Tab. 4.3.

Tab.4.1 - Line set of the IEEE 30-bus system

Line No.	Start bus	End bus	Admittance	F_l^{max}
1	2	1	0.0575	120
2	3	1	0.1852	120
3	4	2	0.1737	120
4	4	3	0.0379	120
5	5	2	0.1983	120
6	6	2	0.1763	120
7	6	4	0.0414	120
8	7	5	0.116	120
9	7	6	0.082	120
10	8	6	0.042	120
11	9	6	0.208	120
12	10	6	0.556	120
13	11	9	0.208	120
14	10	9	0.11	120
15	12	4	0.256	120
16	13	12	0.14	120
17	14	12	0.2559	120
18	15	12	0.1304	120
19	16	12	0.1987	120
20	15	14	0.1997	120
21	17	16	0.1923	120
22	18	15	0.2185	120
23	19	18	0.1292	120
24	20	19	0.068	120
25	20	10	0.209	120
26	17	10	0.0845	120
27	21	10	0.0749	120
28	22	10	0.1499	120
29	22	21	0.0236	120
30	23	15	0.202	120
31	24	22	0.179	120
32	24	23	0.27	120
33	25	24	0.3292	120
34	26	25	0.38	120
35	27	25	0.2087	120
36	27	28	0.396	120
37	29	27	0.4153	120
38	30	27	0.6027	120
39	30	29	0.4533	120
40	28	8	0.2	120
41	28	6	0.0599	120

Tab.4.2 - Generator and load set of the IEEE 30-bus system

No.	Bus	Power	minPower	maxPower
1	1	50	0	100
2	2	45	0	100
3	5	45	0	100
4	8	45	0	100
5	11	45	0	100
6	13	31.7	0	100
3	3	-2.4	-2.4	0
4	4	-7.6	-7.6	0
5	5	-94.2	-94.2	0
6	6	0	0	0
7	7	-22.8	-22.8	0
8	8	-30	-30	0
9	9	0	0	0
10	10	-5.8	-5.8	0
11	11	0	0	0
12	12	-11.2	-11.2	0
13	13	0	0	0
14	14	-6.2	-6.2	0
15	15	-8.2	-8.2	0
16	16	-3.5	-3.5	0
17	17	-9	-9	0
18	18	-3.2	-3.2	0
19	19	-9.5	-9.5	0
20	20	-2.2	-2.2	0
21	21	-17.5	-17.5	0
22	22	0	0	0
23	23	-3.2	-3.2	0
24	24	-8.7	-8.7	0
25	25	0	0	0
26	26	-3.5	-3.5	0

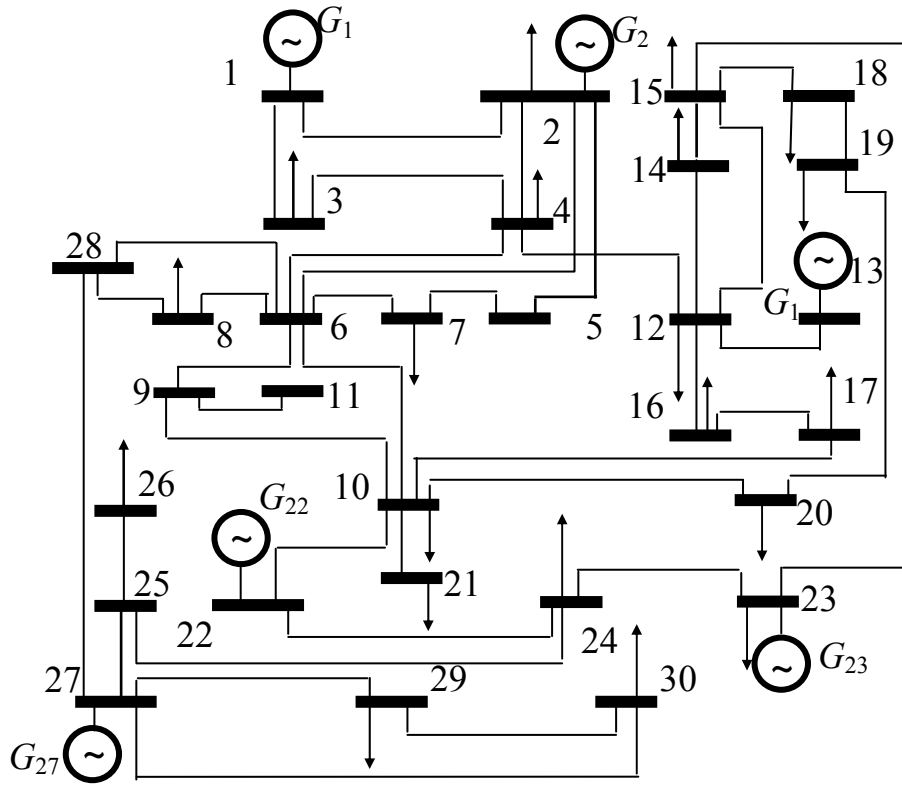


Fig.4.3 - IEEE 30 bus system

Input of the defense/attack actions

The attack and defence cost of the lines and nodes are shown in Tab.4.3. The successful destroyed rate with/without protection of the power system component are respectively $\beta_i=0.2$ and $\alpha_i=0.8$; the load shedding evaluation factor $\gamma_j=10$.

Tab 4.3 – Budget data of attack and defense *

Attacker	Budget	60
	Attack single line cost	26
	Attack single bus cost	60
Defender	Budget	50
	Defend single line cost	20
	Defend single bus cost	50

Equilibrium

In the game, each of the two sides will evaluate their strategies based on the action of their counterpart. The attack and the defense actions are viewed as a potential move for the specific context, which is defined by the configuration of the power system and the budget of the players. The equilibrium of the game in the base case is described in Tab.4.4, in which, at the equilibrium the attacker will attack the buses 1 and 2 with the probability 0.8826 and 0.1174 respectively, and as the countermeasure to fix the equilibrium, the defender will defend lines 35 and 33 with the probability 0.9995 and 0.0005. The defender is not going to defend the buses 1 and 2, although they are more likely to be attacked, because the equilibrium is the outcome of the interaction, if the defender doesn't take the action defined at the equilibrium, for instance to defend buses 1 and 2 instead of lines 33 and 35, the attacker will also change his mind, namely buses 1 and 2 will possibly not be the target of the attacker as well. The expected payoff can be considered as a metric to

*value are in arbitrary monetary unit

provide an overall index for describing the security level of the malicious attack. The expected payoff of the attacker is 1253.6, which is defined by the probability of the actions taken and the corresponding payoff taking into account the cost of the actions and the loss of load. Moreover, as a result of the zero sum game representation, the expected payoff of the defender is the negative payoff of the attacker.

Tab.4.4 - Mixed strategy equilibrium at the original state

Attacker	Attack probability	Bus	1	0.8826
			2	0.1174
		Line	-	-
	Expected Payoff		1253.6	
Defender	Defense probability	Bus	-	-
			35	0.9995
		Line	33	0.0005
	Expected Payoff		-1253.6	

Payoff sensitivity to the defense action

After the base case is obtained, in term of equilibrium with a givens set of defense and attack actions, the information obtained can be exploited, by the defender, to implement defense action that would lead to a new state. Tab.4.4, Tab.4.5, Tab.4.6 Tab.4.7 report under each state, the probability distributions of being attacked and defended to the components along with the corresponding payoffs.

From the Tab. 4.4, Tab. 4.5, Tab. 4.6 and Tab. 4.7, we see that with the non-zero probability defense action implemented, the equilibrium will be changed, and the distribution of the probabilities of the attack and defense will be re-allocated. The results shows numerically that the more defense action are taken, the more the attacks distribution is disperse,. The probabilities of the various attack and defence actions at the equilibrium provide an assessment of which component will be more likely to be attacked or defended.

Tab.4.5 - Mixed strategy equilibrium with lines 35 and 33 defended

Attacker	Attack probability	Bus	1	0.2999
			2	0.2999
		Line	5	0.4002
			9	0.4002
	PayOff		856.8	
Defender	Defense probability	Bus	1	0.4386
			2	0.4386
		Line	5	0.1228
			9	0.1228
	PayOff		-856.8	

Tab.4.6 - Mixed strategy equilibrium with lines 5 and 9, buses 1 and 2 defended

Attacker	Attack probability	Bus	5	0.1017
		Line	8	0.2566
			33	0.2566
			36	0.2566
			37	0.2566
			38	0.2566
			39	0.2566
		41	0.2566	
	PayOff		548.41	
Defender	Defense probability	Bus	5	0.3336
		Line	8	0.1904
			33	0.1904

			36	0.1904
			37	0.1904
			38	0.1904
			39	0.1904
			41	0.1904
	PayOff		-548.41	

Tab.4.7 - Mixed strategy equilibrium with bus 5, lines 8, 33,36,37,38,39 and 41 defended

Attacker	Attack probability	Bus	-	-
		Line	1	0.0965
			2	0.0481
			4	0.0484
			15	0.2701
			26	0.1918
			29	0.2701
			30	0.2675
			31	0.2679
			32	0.2695
		40	0.2701	
PayOff		568.43		
Defender	Defense probability	Bus	-	-
		Line	1	1
			2	0.1904
			4	0.1904
	PayOff		-568.43	

The payoff variation with different defense actions implemented is shown in Fig.4.4. From the defender point of view, the payoff increases fast at the beginning when defense actions are taken; it reaches a maximum value at the third action, After that, the defender's payoff actually decreases, if additional defense actions are taken. In this example, to defend lines 33, 35, 5, 9 and buses 1 and 2 is the optimal action for the defender willing to maximize its payoff.

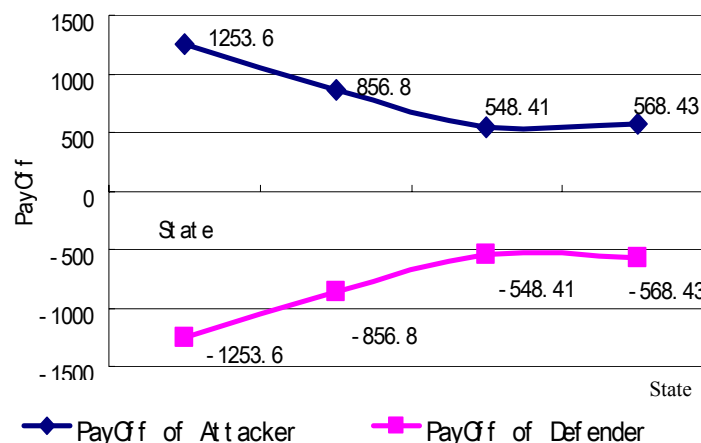


Fig.4.4 - Payoff variation with the defense actions implementation

Payoff sensitivity to the resources allocated by the players

The payoff variation with respect to the variation of the budgets of the defender and attacker is reported in Fig. 4.5.

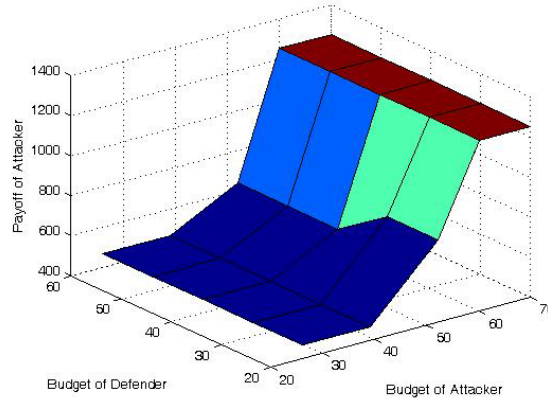


Fig.4.5 - Payoff sensitivity to the variation of the budget of defender and attacker

The variation of the budget of both the defender and attacker will surely impact the result of the interaction between the attacker and defender. This is because the defense and attack action sets are determined by the corresponding budgets allocations. In Fig. 4.5 we see that, when the budget of the attacker increases from 30 to 60, the payoff of the attacker increases rapidly showing the amplifier effect of the infrastructure. On the contrary, an increase of the defense budget (e.g. from 25 to 60) is much less effective to curb the attack effects. In other words, the payoff of the attacker is very sensitive to the budget of the attacker, but much less sensitive to the budget of the defender. This implies that the defender must allocate much more resources in order to be sure to achieve some significant impact of the defense measures deployed.

5. MODELING OF COORDINATION/COOPERATION UNDER MALICIOUS ATTACKS WITH MAS

5.1 MAS APPLICATION TO COORDINATION/COOPERATION MODELING

Artificial Intelligence (AI) methods are used to tackle complex, realistic, and large-scale problems. One such method which found successful recent application in complex problem solving is the multi-agent approach. This section explores in which way this method may be applied to modeling malicious attacks to critical infrastructures.

5.1.1 DEFINITIONS

An agent is an abstract or physical autonomous entity which performs a given task using information gleaned from its environment to act in a suitable manner so as to complete the task successfully. The agent should be able to adapt itself based on changes occurring in its environment, so that a change in circumstances will still yield the intended result.

An agent is rational if it always selects an action that optimizes an appropriate performance measure, given what the agent knows so far. The performance measure is typically defined by the user (the designer of the agent) and reflects what the user expects from the agent in the task at hand. A rational agent is also called an intelligent agent.^[35]

The thing an agent interacts with, comprising everything outside the agent, is called the environment. The collective information that is contained in the environment at any time step t , and that is relevant for the task at hand, will be called a state of the environment.

Assume that an agent interacts with its environment at each of a sequence of discrete time points $t = t_0, t_1, \dots, t_n$. Let $S = \{s_1, s_2, s_3, \dots, s_n\}$ be the finite set of possible states of the environment and $A = \{a_1, a_2, a_3, \dots, a_m\}$ be the finite set of admissible actions the agent can take. At each time step t , the agent senses the current state $s_t = s \in S$ of its environment and on that basis selects an action $a_t = a \in A$. As a result of its action, the agent receives an immediate reward r_{t+1} , and the environment's state changes to the new state $s_{t+1} = s' \in S$.

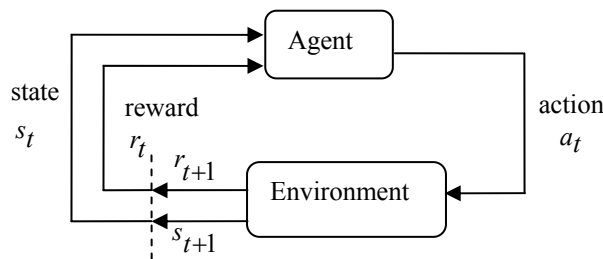


Fig.5.1-Agent's interaction with the environment

A Multi-agent system is composed of a group of autonomous agents. Each agent has its own local view of the world and its own goals. The agent will adjust its behavior based on a heuristic learning algorithm so as to obtain a realistic outcome of the system. The main difference between the Game Theory and the Multi-agent approach is that Game Theory algorithms assume that the transition and reward

function is known, while Reinforcement Learning algorithms used in the Multi-agent approach only receive observations about the transition and reward function and learn by experience.^[35]

Reinforcement learning (RL) is a generic name given to a family of techniques in which an agent tries to learn a task by directly interacting with the environment. RL techniques may be successfully applied to finding optimal control policies for a single agent operating in a stationary environment, specifically in the frame of a Markovian decision process (the current state provides a complete description of the history before and the distribution of future states only depends on the current state but not any past states). Agents are required to act in the environment in order to gain observations about transitions and rewards. The field of single-agent RL is nowadays mature, with well-understood theoretical results and many practical techniques.^[36] On the contrary, the field of multi-agent reinforcement learning in which many agents are simultaneously learning by interacting with the environment and with each other, is less mature. The main reason is that many theoretical results for single-agent RL do not directly apply in the case of multiple agents.^[35]

There are various reinforcement learning algorithms as Q-Learning, Opponent Modeling Q-Learning, Actor-Critic, Gradient descent, Win or Learn Fast (WoLF), which can be used for the agent to make response to the change of the environment. In Q-Learning, a table of values is updated while playing a stochastic game. This Q-table can be used to choose actions that will maximize expected discounted rewards.^[36] The Opponent Modeling Q-Learning method is based on the Q-Learning method and records the probability distribution of opponent actions in each state by observing the actions of the other player. In actor-critic systems, there are two components to the reinforcement-learning system, the critic learns values, and the actor learns policies. At any given time, the critic is learning the values for the Markov chain that comes from following the current policy of the actor. The actor is constantly learning the policy that is greedy with the respect to the critic's current values. Gradient descent is an optimization algorithm. To find a local minimum of a function using gradient descent, one takes steps proportional to the negative of the gradient (or the approximate gradient) of the function at the current point. If instead one takes steps proportional to the gradient, one approaches a local maximum of that function. In our model, the independent learning method has been implemented because it realizes a good compromise between computational efforts and accuracy of results.

Different criteria for decision making may be suitable for different scenarios; in our model we have chosen the widely used criterion based on the choice of the maximum Q-value for each agent in the independent learning scenario. Moreover there are also various criteria for decision making such as Minimax-Q, Nash-Q, Friend or Foe, CE-Q etc. For zero-sum stochastic games, Minimax-Q is based on updating the utility values by the minimax of Q values so that an agent can maximize private utility based on minimizing the utility of the opponent. Nash-Q updates the utility values based on some Nash equilibrium in the game defined by the Q-values. For Friend or Foe, it is more informative to view FoF as two algorithms, each applying in a different special class of stochastic games. The Friend class consists of stochastic games in which, throughout the execution of the algorithm, the Q-values of the players define a game in which there is a globally optimal action profile. The Foe class is the one in which the Q-values define a game with a saddle point. CE-Q is similar to Nash-Q, but instead uses the value of a correlated equilibrium to update the utility values.

5.1.2 MODELING A CONFLICT FRAMEWORK WITH MULTIAGENT SYSTEMS

The Multi-agent approach allows to model effectively conflict contexts . Agents behave in a bounded rational manner. They learn from the environment and by experience so as to find the best strategy option for each agent. Therefore in our case, each agent in the system will judge the situation based on the environment with particular attention to its experience:

- Attacker Agent (e.g. terrorists) will evaluate the effect of its attacks based on the records (success or failure with respect to a specific attack target, the influence on economy or psychology of common people or the achievement of their political purpose) so as to decide upon the next move. A model about the decision strategy and the knowledge of the opponent, especially for defender, would make the simulation more realistic.

- Defender agent (e.g. the government and relevant entities) will on one hand check the past behavior of the attackers and on the other hand evaluate the environment where potential attacks may be deployed against specific targets. A model about the decision strategy of the attacker based on its knowledge or information would be helpful for better decision.

- Sufferer agent – who suffers direct consequences of attacks – may react by evaluating the impact of behavioural changes with reference to a specific infrastructure reacting to a specific attack (e.g. by changing to another transport system, less water consumption...) and in terms of pressure/support to the government. The reaction of the sufferer would be transformed as rewards for both the attackers and the defenders in some way to influence their decisions; however this agent may not take part in the struggle about the infrastructure directly.

As shown in Fig.5.2, the infrastructures are represented by the gray octagon in which the vertices represent different potential attacking targets. The defender agent decides the defending strategy which is represented by the green circle in broken lines based on rational decision. The attacker agent makes decision about which targets and how to attack based on rational decision. Although the attacker may only choose to attack some specific points as represented by the red vertices, this attack may influence the function of the whole infrastructure. Then the suffer agent will be injured by not only the targets attacked but also the other targets as shown by the grey arrows from all vertices to the suffer agent. In this way, the attacking effect is amplified. Attackers and defenders influence the sufferer agent(s) through the infrastructures. Then the sufferer agent will make feedback which is represented by the blue arrows to the attacker agent and the defender agent to influence their future decisions.

In that interplay, a specifically constrained network such as a power system, a water supply system, etc., will be evaluated for the weak points to have the highest possibility to be attacked according to the actual situation and system records, which can be modeled as the environment of all agents and then the transition and reward analysis will be carried out to predict the next step.

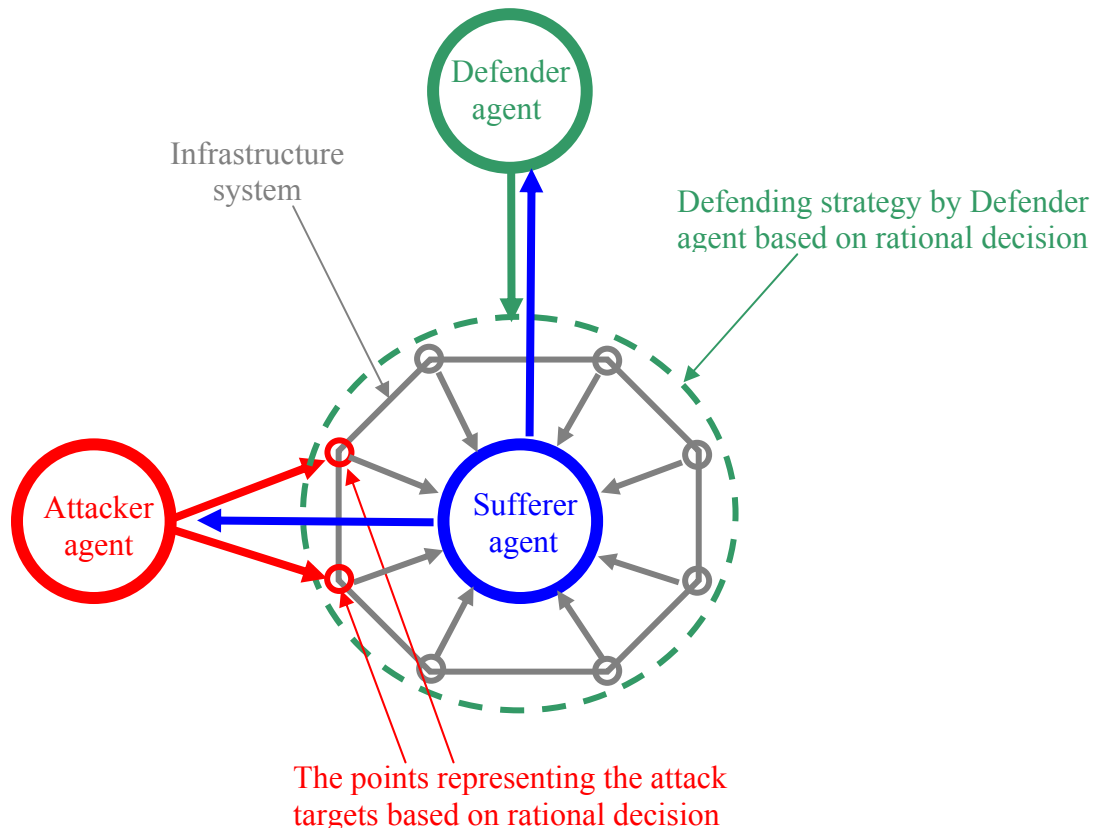


Fig.5.2 - Interaction within the agents involved in terrorism attack

5.1.3 MULTI-AGENT REPRESENTATION FOR CRISIS MANAGEMENT AND INFORMATION IMPACT ANALYSIS

Different situations and aspects can be captured resorting to MAS. Two particularly important aspects are the related coordination processes among various entities and the impacts of the availability of information under emergency conditions.

The growing complexity of the network structure, the restructuring and deregulating of power systems all make it unreasonable to keep considering the defender of power systems as a single united entity. Inappropriate interactions among all stakeholders in the defending process will magnify the influence of attacks and become a new source of vulnerability. So the coordination of different System Operators (SOs) in an interconnected power system is an important issue in defense against malicious attacks.

When analysing power system security against malicious attacks, the attention should not only focus on the interactions between the defenders and attackers, but also on the coordination among the stakeholders of the defender. At the same time, the effect of coordination depends seriously on the availability of different information. According to the UCTE operation handbook^[38], during emergency situations there should be exchange of information between SOs about systems' conditions next to the borders: topology, weak points in the network and potential risk of operation. Each SO has to make available real-time information about relevant parts of its own system to other neighbouring SOs. So the communication is very important for the relevant control entities to achieve successful joint control target.

To have a clear insight of this problem, we should divide a power system into two tightly interconnected layers, the physical layer and the operating management one. The management layer can be further sub-divided into a coordination sub-layer

and an information sub-layer. The relationship between all these layers is shown in Fig.5.3.

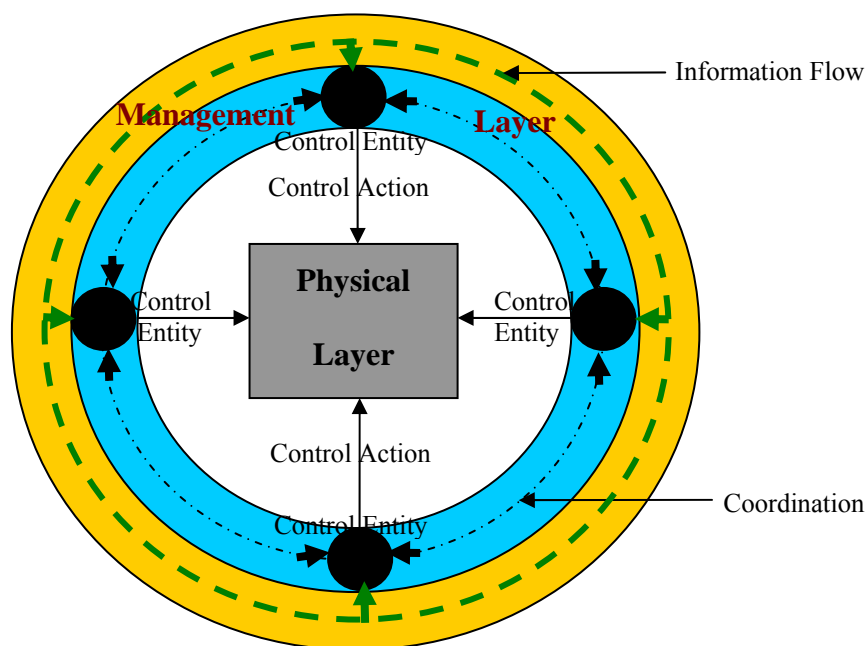


Fig.5.3-Physical/Management layers interactions

All the relevant control entities, that are the entities in charge for each SO to operate the system, pertain to the operating management layer. Each of them may have a special role in the control mechanism and can only influence limited part of the physical layer. The physical layer is composed by the system lines and buses on which the power actually flows. The control entities will implement their control actions on the physical layers, as a reaction to malicious attacks, resorting to the information they get from the information sub-layer.

Coordination schemes under emergency conditions

As rationality is an important feature of an agent, it is reasonable to resort to multiple agents to represent different control entities in the management layer with their own role, target and interest. In this way, we can simulate the mechanism of coordination between control entities and its influence on the control results by the coordination between agents and the output state of the environment.

In multi-agent system, there is still no universally best coordination mechanism^[39]. Each coordination mechanism should be selected according to the characteristics of the tasks in hand.^[39] In coordination of interconnected power systems, the SOs have equal positions with no priorities to make decision and there is no direct central decision making for them. Each SO is a self-interest entity but also has motivation to help other peers. The time scale of control under emergent situation is short. All these characteristics make some mechanisms with central decision, unequal priorities^[40] or long or medium term planning^{[41][42]} not appropriate to this problem.

SOs are rational agents. They act on their own interest with a cooperative attitude, because their own system security depends on the others. The security of the whole interconnected power system is beneficial for each subsystem, so all SOs are willing to be cooperative to some extent. But at the same time, every SO cares more

for its own system security and would not like to be much constrained by collaboration rules and procedures. These problem features call for a methodology able to reconcile self-interest with cooperation. This can be achieved by an appropriate balance between cooperation and self-interest in the design of rational agents performance measure.

Information impacts under emergency conditions

Information plays a key role under emergency condition since, especially under emergency, the decision assumed relies on the data available and their completeness. However as the configuration of the control entities in power system and the actual management mechanisms are very complex, the communication mechanism and relevant information depend on different roles of different entities and their relationships. Control layers, their relationship, and the relevant information flows among them can be schematically represent as follows (fig 5.4)

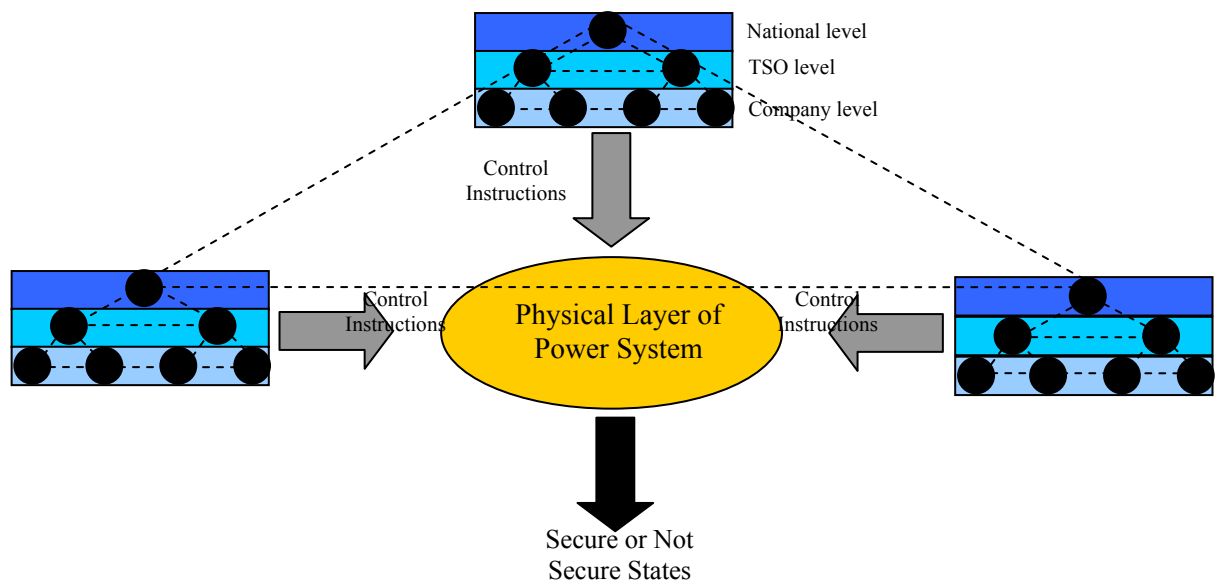


Fig.5.4-Configuration of entities and their communication

In Fig.5.4, as an example, we may divide the control entities into three levels that may be more suitable for representing the situation in Europe. The first national level is related to the entities representing the systems of different countries. Under it, the second level is for the different TSOs operating under the national level. The third level may be for the companies distributed in the network managed by the TSO. The communication among different entities is represented by broken lines. All these entities take operational decisions on the physical power system based on their own analysis of the information they can get. And the output state of the power system results from the joint operations of these entities.

In multi-agents system, each agent can only perceive limited information about the environment. To achieve better cooperation, they also need communication for more information about the environment. So still using multiple agents to represent the entities at different levels, we can simulate the communication between different entities as the communication between agents. But as the location and role of the entities are different, the corresponding agents may have different structure, target and interest. That makes meaningful to simulate which information may be critical for

some potential malicious attacks or what would be the consequence if some communication is disabled by malicious attacks analyzing different scenarios.

5.2 EXAMPLE OF MAS MODEL FOR INFORMATION IMPACTS IN COORDINATION

The model deals with a set of SOs running different interconnected power systems; the systems are interconnected via tie-lines and the malicious attack may target to those lines and/or to lines that are internal to the systems. Each SO has full control on the generation and loads in its own system; it can get the measures on the state (line power flows) on its system and, eventually, get also information about some of the states of the neighbor systems. Different levels of information about the state may be available to different operators at different time points both due to specific policy decisions, related to the international agreements (bilateral, or by the UCTE, the NORDEL and international TSOs associations alike), and to monitoring equipment failures due both to accidental faults and deliberate manipulation (e.g. via cyber attacks). Under malicious attacks each operator may chose different behaviors, according to its utility and based on available information and the internationally agreed rules of behaviour ; it may focus just on its system trying to maximizing a measure of the its system welfare (“individual behavior”) or may want to contribute to the welfare of the all interconnected system, including all the grids of the other operators (“social behavior”). In the first case the reaction under attacks will be characterized by a lack of coordination while in the second case we have full coordination; of course different levels of coordination within these two extremes are possible. The proposed model aims to study the outcomes of difference choices in terms of coordination under various scenarios characterized by different levels of information available.

5.2.1 INDIVIDUAL AND SOCIAL RATIONALITY

The different attitudes in terms of attention to the welfare of the overall system - or only to their own system specific welfare - can be modeled resorting to the notion of individual and social agent ^[43]. *An individually rational agent* is an agent who focuses only on its own (individual) utility when deciding which action to perform. *A socially rational agent* is an agent who also considers the utility of other agents in deciding which action to perform.

We will use the notion of expected utility of actions in deriving a more descriptive notion of choice within a multi-agent environment. From the aforementioned principle of social rationality, to calculate the expected utility (U_i^E) of an action α implemented by agent i , the agent needs to combine (using some function f) the individual utility (U_i^I) afforded to itself which performs α and the social utility (U_i^S) afforded to the overall system when α is executed^[43]:

$$U_i^E(\alpha) = f(U_i^I(\alpha), U_i^S(\alpha)) \quad (5.1)$$

The individual utility is a measure of the welfare of the agent (operator) related to its systems while its social utility is a measure of the welfare of the global system that it is willing to consider. The social utility is based on different “social relationships”, in terms of power exchange with the other SOs, in which the agent is engaged.

Let the set of social relationships in which a particular agent (i) is engaged be denoted by the vector $\lambda^i = [\lambda_1^i, \lambda_2^i, \dots, \lambda_n^i]$. To each relationship we associate a vector

of coefficient $\varphi^i = [\varphi_1^i, \varphi_2^i, \dots, \varphi_n^i]$ with $0 \leq \varphi_j^i \leq 1$ and $\sum_{j=1}^n \varphi_j^i = 1$ that weight the importance of each of these relationships. And $U_j^S(\alpha)$ is the “social relationship utility” which is the utility afforded to the agent in λ_j^i by the execution of α .

Function f in (5.1) can be written as:^[43]

$$U_i^E(\alpha) = k_1 \cdot U_i^I(\alpha) + k_2 \cdot \left(\sum_{\forall j \in \lambda^i} \varphi_j^i U_j^S(\alpha) \right) \quad (5.2)$$

where k_1 and k_2 , with $k_1 + k_2 = 1$, are two coefficients devoted to weight the individual and social utilities on the expected utility of an action α .

5.2.2 MAS MODEL FOR COORDINATION UNDER VARIOUS INFORMATION SCENARIOS

In the following paragraphs, we will introduce the MAS model in terms of different main aspects to have a clearer insight for the configuration of the model. In this way, the mechanism of the simulation can be understood easily.

Overall System Structure

The system is composed by n different subsystems (S_1, S_2, \dots, S_n) interconnected by tie-lines with each other. We define n different agents to represent the operators of each subsystem.

Each agent will:

- Sense information from its local system to simulate the real situation that each OS can only collect information of local system directly;
- Determine what action to perform on its local system, based on its utility function.

System States

The controlling process of multi-agent system can be considered as a transition process. Each agent distinguishes and judges the state according to its own perceptions and implement actions to transit to the desired state.

There are some traditional and classic methods to classify the power system states^[44]. But in this model, according to the point of view of agents and the control process, we simply consider:

- Secure states: when no line is overloaded.
- Emergency states: when at least one line is overloaded after an attack.

The states transition is shown in Fig.5.5. The control process of agents in this model is to move the state of the system from *Emergency* to *Secure*. Both *Secure* and *Emergency* states are composed of different operative configurations characterized by different power flows, generation and load distributions.

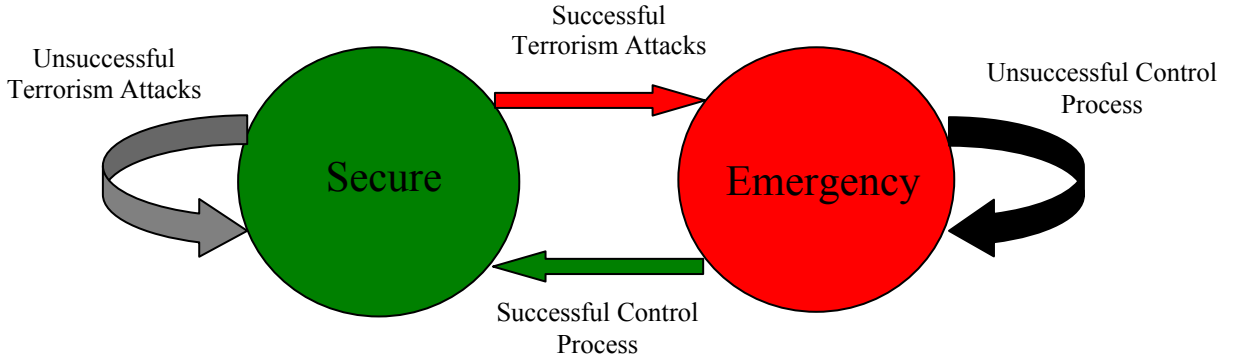


Fig.5.5-States Transition

Action Set

To remove the security contingency, we assume that all the operating agents can only select to shed loads at the buses of their own territory. Since at different operative configuration, the distributions of loads at all buses are different, the available actions at different configurations are different.

We assume that the set of control actions is discrete according to the nature of some of them and to the possibility to make the other discrete as well. In the local subsystem, if there are m buses whose loads are possible to be shed, we define a vector A named as *action scheme* which consists of m elements. Each element has two possible values 0 (load on this bus is not to be shed) or 1 (load on this bus is to be shed). For example $A = \{1, 0, 0, \dots, 0\}$ means that only the load on bus 1 is to be shed.

Attacking Pattern

We just consider attacking patterns consisting of cutting off some tie-lines or internal transmission lines. One attacking pattern may include several attacked lines. Since our research purpose is the coordination under malicious attacks, the attacking pattern is fixed when to make simulation of coordination.

Learning Method

We assume the attacking pattern is fixed and at the beginning of every time step the system is in one of the *Secure* operative configurations. After the fixed attack happens, the system would be transferred to one *Emergency* operative configuration. Each agent will try to control the system back to some *Secure* operative configuration, by choosing an action scheme to implement. No matter if the operative configuration of the system has been moved to *Secure*, at the end of this time step or not, the agent will receive a reward, that is a measure of the utility got from its action, as the effect for its action. In the next time step, this process will be repeated.

Although there is no direct interference in the coordination of interconnected power system, some coordinating organization (such as UCTE) would make some coordinating rules which can restrict the selections of agents. Whatever the contents of the rules are, the final effects should be the restriction on selection of actions. Some combinations of actions are forbidden according to the rules in some specific situations.

We assume that j is the combination of actions which is composed of n different actions by n agents $(\alpha_1 \alpha_2 \dots \alpha_n)$. \mathcal{J} is the set of all possible combinations. \mathcal{J} is the set that approved by the rules and \mathcal{J} is the set that forbidden by the rules.

According to this, we apply the classic Q-learning method to independent learning with constraints \mathcal{J} . For each agent i , the learning formula is:

$$Q_{t+1}^i(s, \alpha_i) = Q_t^i(s, \alpha_i) + \beta[R_i - Q_t^i(s, \alpha_i)] \quad (5.3)$$

where $i = 1, 2, \dots, n$ and $j = (\alpha_1 \alpha_2 \dots \alpha_n) \in \mathcal{J}$

In the classic Q-learning theory, the learning rate β must fulfill some conditions to guarantee its convergence ^[45]. But this is based on the single agent scenario where the state transition probability and reward probability are deterministic by states of environment and its actions. But in multi-agent independent learning, the other agents included in the environment are also learning and adjusting their decisions which make the environment not deterministic. The convergence of the learning process depends on that the learning process of other agents would settle down ^[37]. So we fix β as 0.9 based on our empirical simulations. ^[46]

Initial values and dynamic exploration

When multiple equilibria exist, the selection of equilibrium is always a boring problem for multi-agent reinforcement learning. Here we refer to the initial values, dynamic exploring rate and constraints by \mathcal{J}^+ to improve the situation in our independent learning model.

The agents use greedy action selection with an exploring rate to explore other actions. The initial values are the starting evaluations of all potential actions to be exploited. The less the exploring rate is, the more the learning process will follow the direction of initial values. So the initial values can be considered as the sequence of wills about which load to be shed when the operator has no further knowledge about the physical situation in the networks. When the exploring rate begins from zero and increases slowly, the learning result may be a feasible action scheme which is much “closer” to the initial wills.

In this model, we assign initial values to different action schemes according to their quantity of loads to be shed as the initial wills of operators when they have no further knowledge about the physical behaviors of the system. The less quantity of loads to be shed an action scheme has, the higher value it would be assigned. The exploring rate begins from zero and increases to an up limit 0.2.

To assure that the learning process stops at a real equilibrium; we take use of multiple convergences. Every time when all Q-values converge, these Q-values will be considered as initial values and the learning process restarts again until the two consecutive convergences of Q-values bring to the same decisions in terms of action schemes.

Utilities

To reflect the security situation of the model system, we use overload rate of lines to calculate the utilities of each agent for their actions. \mathcal{L} is the set of all lines. For one line l of \mathcal{L} , if its active power flow is P^l and maximum power flow limit is P_{max}^l , then the utility for this line is :

$$U^l = \begin{cases} 0 & (\text{If } P^l \leq P_{max}^l) \\ (P_{max}^l - P^l) / P_{max}^l & (\text{If } P^l > P_{max}^l) \end{cases} \quad (5.4)$$

It should be emphasized that the utility is negative when the line is over loaded, so the purpose of the agents is to maximize this utility as coherent with the normal learning situation for agents.

If \mathcal{I} is the set of internal lines whose both terminal buses are all in the local territory for *agent i*, \mathcal{T}_i is the set of tie-lines for *agent i* whose one terminal bus is in the local territory and the other is in another territory. Then the individual utility for *agent i* is:

$$U_i^I = \sum_{l \in \mathcal{I}_i} U^l + \sum_{l \in \mathcal{T}_i} 0.5U^l \quad (5.5)$$

As discussed, an individually rational agent would only focus on the utility of its actions for itself, while a socially rational agent would consider both the utility for itself and the utility for other agents from its actions. Hence, for socially rational agents, the calculation of expected utility can be expressed as:

$$U_i^E = k_1 * U_i^I + k_2 * (\varphi_1^i * U_1^I + \varphi_2^i * U_2^I + \dots + \varphi_n^i * U_n^I) \quad (5.6)$$

Where U_i^E is the expected utility for *agent i*, k_1 is the weight at which *agent i* considers its own utility, k_2 is the weight at which *agent i* considers the utilities of its social relationship. $k_1 + k_2 = 1$. $\varphi_1^i, \varphi_2^i, \dots, \varphi_n^i$ are the weights which shows how much *agent i* considers all other agents should occupy in its social relationship. $\sum_{k=1}^n \varphi_k^i = 1$. If *agent n* has no social relationship with *agent i*, then $\varphi_n^i = 0$.

The evaluation of φ depends on how tight the interaction between the two agents is in the current time step. We use the absolute value of power exchange between the two parts as the parameter to evaluate the interaction. If the interaction between *agent i* and another agent is more active, then *agent i* would like to consider the overload rate of this agent more important. If $P_k^i (k = 1 \dots n)$ is the absolute value of active power flow exchanged at tie-lines between *agent i* and *agent k*, then calculations of $\varphi_1^i, \varphi_2^i, \dots, \varphi_n^i$ can be expressed as:

$$\varphi_k^i = P_k^i / (P_1^i + P_2^i + \dots + P_n^i) \quad (k = 1 \dots n) \quad (5.7)$$

Then the calculation of reward for a socially rational agent is:

$$R_i = \begin{cases} U_i^E & (\text{if } U_i^E < 0) \\ (M_i - L_i) / M_i & (\text{if } U_i^E = 0) \end{cases} \quad (5.8)$$

But the calculation of reward for an individually rational agent can be expressed as:

$$R_i = \begin{cases} U_i^I & (\text{if } U_i^I < 0) \\ (M_i - L_i) / M_i & (\text{if } U_i^I = 0) \end{cases} \quad (5.9)$$

M_i is a constant which is the maximum quantity of loads to be shed in each of all possible action schemes in the subsystem of SO *i*. L_i is the sum of loads shed by SO *i* in its subsystem in the implemented action scheme.

Information Scenarios

Different levels of information available would influence the effect of coordination. In our model, the calculation of utilities is based on the information of active power of transmission lines. For different scenarios of information available, the calculating results would depend on how much information about neighbors each agent can get.

In this model, we just consider two extreme scenarios:

- *Full information*: information about active power of all transmission lines of neighbors is available. This scenario is simulated by socially rational agents.
- *No information*: no information about active power of transmission lines of neighbors is available. This scenario is simulated by individually rational agents.

5.2.3 CASE STUDY AND RESULTS

We apply, for illustrative purpose, the model introduced in the previous section to a 34-bus system to analyze the coordination of SOs in different information scenarios to the aim of :

- analyzing the effect of the coordination by socially rational agents as a method to make balance between cooperative behaviors and self-interested behaviors;
- analyzing the impact of information from the results of two different information scenarios;
- analyzing the different information sensitivity of operative configurations to indicate their different dependencies for information.

Sample system

The sample 34-bus system is composed of three interconnected subsystems shown in figure 5.6. In this system, three different subsystems are controlled by three different SOs (SO1, SO2 and SO3). Line data, generation and load data are respectively given as Tab. 5.1 and Tab.5.2.

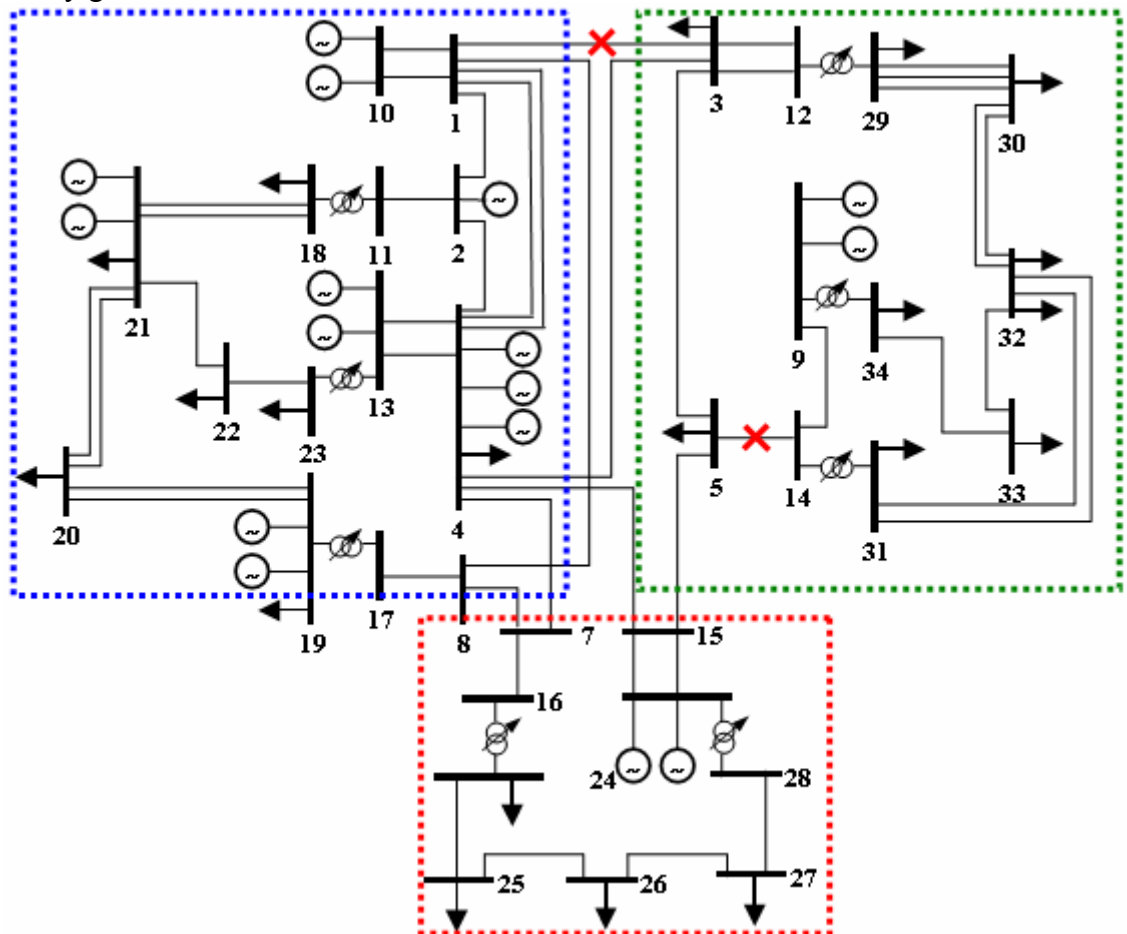


Fig.5.6-Structure of Sample System

Tab.5.1 – Line data

Line NO.	Start bus	End bus	Admittance[p.u.]	P_l^{max} [p.u.]
1	1	2	0.05062	2.286
2	1	3	0.05785	3.0
3	1	4	0.05785	2.286
4	1	4	0.08161	2.286
5	1	8	0.12934	2.286
6	1	10	0.00413	2.477
7	1	10	0.00413	2.477
8	2	4	0.05062	2.286
9	2	11	0.00413	2.286
10	3	4	0.13843	2.286
11	3	5	0.20041	2.286
12	3	12	0.00413	2.286
13	3	12	0.00413	2.286
14	4	15	0.05114	2.286
15	4	7	0.06818	2.286
16	4	13	0.00413	2.286
17	4	13	0.00413	2.286
18	5	15	0.0657	2.477
19	5	14	0.00413	2.286
20	6	15	0.00413	2.286
21	6	15	0.00413	2.286
22	7	8	0.06674	2.286
23	7	16	0.00413	2.286
24	8	17	0.00413	2.286
25	9	14	0.08161	2.286
26	30	29	0.04756	1.039
27	30	29	0.04756	1.039
28	30	29	0.04756	1.039
29	32	30	0.04756	1.039
30	32	30	0.04756	1.039
31	32	31	0.04756	1.039
32	32	31	0.04756	1.039
33	34	33	0.092	1.039
34	33	32	0.092	1.039
35	24	25	0.04756	1.039
36	26	25	0.04756	1.039
37	27	26	0.04756	1.039
38	28	27	0.04756	1.039
39	19	20	0.04756	1.039
40	19	20	0.04756	1.039
41	21	20	0.04756	1.039
42	21	20	0.04756	1.039
43	21	22	0.092	1.039
44	18	21	0.04756	1.039
45	18	21	0.04756	1.039
46	22	23	0.092	1.039
47	29	12	0.01033	3.811
48	31	14	0.01033	2.286
49	34	9	0.02066	2.286
50	24	16	0.02066	2.477
51	28	6	0.02066	2.477
52	19	17	0.01033	3.429
53	18	11	0.01033	2.286
54	23	13	0.04132	2.286

Tab.5.2 - Distribution of generations and loads

Bus NO.	Operative Configuration 1		Operative Configuration 2	
	Generation [p.u.]	Load [p.u.]	Generation [p.u.]	Load [p.u.]
1	0	0	0	0
2	1.8	0	1.8	0
3	0	1	0	1
4	0	3.8	0	3.8
5	0	1.8	0	1.8
6	2.4	0	0	0.7
7	0	0	0	0.4
8	0	0	0	0
9	2	0	3.4	0
10	3.4	0	3.4	0
11	0	0	0	0
12	0	0	0	0
13	4	0	4	0
14	0	0	0	0
15	0	0	0	1.0
16	0	0	0	0
17	0	0	0	0
18	0	0.9	0	0.9
19	1.15	0	1.15	0
20	0	1.75	0	1.75
21	2.7	0	2.7	0
22	0	0.6	0	0.6
23	0	0.6	0	0.6
24	0	0.5	0	0.5
25	0	0.5	0	0.5
26	0	0.5	0	0.5
27	0	0.5	0	0.5
28	0	0	0	0
29	0	0.9	0	0.5
30	0	0.95	0	0.55
31	0	0.9	0	0.5
32	0	1.05	0	0.05
33	0	0.6	0	0
34	0	0.6	0	0.3

Input of the model:

We fix the attacking pattern as cutting off two lines between bus1 and bus3 and between bus5 and bus 14.

For simplification of computation, here we only consider two operative configurations in *Emergency* which have two corresponding operative configurations associated via the fixed attacking pattern in *Secure*. The power exchange, in p.u., among all these three parts at the two different operative configurations has been displayed as Fig.5.7.

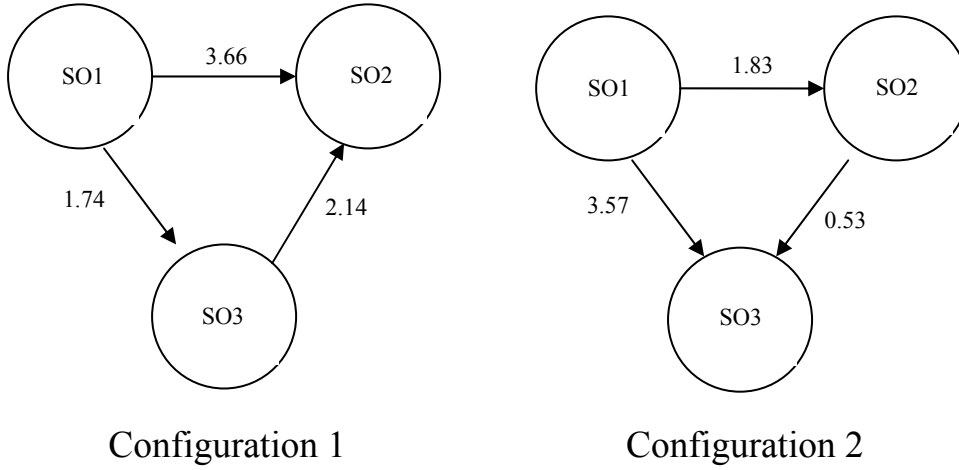


Fig.5.7-Power exchange at different operative configurations (values are expressed in p.u.)

In the learning process, each operative configuration has a fifty percent probability at the beginning of each time step.

We assume that each agent may shed the loads of one or two buses under its control in one action scheme. At different operative configurations, the distributions of loads at all buses are different, so the available action schemes at different operative configurations are different. The values of M_1 , M_2 and M_3 are assigned according to the loads distribution and the rule expressed in last section. We set k_1 and k_2 in formula (5.6) as $k_1 = k_2 = 0.5$ which means attitude of medium extent about individual interest and social interest.

According to the UCTE operation handbook, to require cooperation of other operators to relieve the congestions in its own subsystem, an operator should have devoted all possible internal resources and failed. So we assume such a coordinating rule that after the learning process by individually rational agents, if one agent fails to relieve its own congestions, its action should have been fixed as the one shedding the maximum possible loads in its subsystem during the learning process by socially rational agents. This can be considered as a constraint \mathcal{I} .

Effects of the coordination

For operative configuration 1, the individually rational agents and socially rational agents can get the same action result which is successful to remove all congestions of the interconnected power system (as shown in Tab.5.3).

Tab.5.3 - Results for operative configuration 1

	Scenario of no information (Individually rational agents)			Scenario of full information (Socially rational agents)		
	SO1	SO2	SO3	SO1	SO2	SO3
Bus of shed loads	None	33 34	None	None	33 34	None
Quantity of shed loads [p.u.]	0	1.2	0	0	1.2	0
Over loaded rate of subsystem	0	0	0	0	0	0

For operative configuration 2, individually rational agents fail to remove congestions, while socially rational agents can successfully remove all congestions (as shown in Tab.5.4).

Tab.5.4 - Results for operative configuration 2

	Scenario of no information (Individually rational agents)			Scenario of full information (Socially rational agents)		
	SO1	SO 2	SO 3	SO 1	SO 2	SO 3
Bus of shed loads	No	3	6	22 23	3 5	24
Quantity of shed loads [p.u.]	0	1	0.7	1.2	2.8	0.5
Over loaded rate of subsystem	0	-0.5	0	0	0	0

These two scenarios (configuration 1 and 2) show the effect of coordination on the control results. With full information available, a set of socially rational multi-agents achieve effective coordination in reaction to malicious attacks. They come to an effective balance in between operative behaviors and self-interested behaviors. This result coincides with the characteristics of interconnected power systems where SOs both have to make contributions to overall system security and also try to maintain their individual interests.

Impact of information

For the two different information scenarios, from the different results of operative configuration 2 we can see that the availability of information about other systems would have serious impact on the coordination effect. However in this example, two extreme situations only have been studied. In the real power system, the scenario of available information would be far more complex. Hence this result is only qualitative. To have a clearer evaluation, we need a suitable way to quantify information impact. This is a valuable further research direction.

Information sensitivity

By comparing the results of operative configuration 1 and configuration 2, we also find that information impact is not the same for all operational configurations. For configuration 1, control results are the same for individually and socially rational agents: lack of information makes no impact on coordination of configuration 1 but makes serious impact on coordination of configuration 2. Information impact is case

sensitive. Different operative configurations would have different sensitivity for information in coordination. It would be a valuable research direction to find some way to quantify this sensitivity.

6. CONCLUSION

Recent tragic events point out how malicious attacks to critical infrastructures are a very serious concern to modern societies due to the huge impacts they may bring to the social welfare in many respects. Among those infrastructure power systems, that are the backbone of modern societies, appear as a sensitive target for malicious attacks and the issue along with its implications in terms of possible impacts and defence strategies have not been yet deeply studied and understood.

The present international scenario, prompts for a new approach to power system security able to incorporate the challenge related to the malicious threats in addition to the well know natural threats that have been considered since the beginning of the electric industry; both physical and cyber attacks need to be considered due to their different specificities. Not so much work can be found in literature about this topic and practically no applicative tools have been devised and effectively employed. In this respect the additional work outlined by this report is of the utmost importance and is surely needed.

Mainly two aspects need to be addressed. The risk assessment of the menace related to malicious attacks to power systems is a key point for pointing out the most critical components of the infrastructure and for devising the most appropriate defence plans, choosing the optimal allocation of the available resources. Moreover, after than an attack has been implemented, the best strategy for managing the post-attack scenario, with special reference to the coordination and cooperation among the various entities that are in charge for operating the power systems, need to be planned and verified in advance

The aspect considered need a proper theoretical framework for modelling the issues described and, based on that framework, proper simulation tools, able to provide scenario assessment with sensitivity analysis of the relevant factors involved (information availability, budget constraints,...) need to be developed and applied by system operators and governmental body as an aid in decision making processes.

We provide a conceptual framework for representing the malicious attack to which ever critical infrastructure, able to capture its specificity. With respect to the natural and accidental threats that have been traditional considered in the protection of power systems, the new malicious threats are different in their nature since they are based on a strategic interaction between different players; that interaction is a key-point for modelling the menace and devising protective strategies.

In this report, the problem of risk assessment in power systems is addressed resorting to a game theory based approach that proved to be effective in modelling the strategic interaction. Particularly, the likelihood of attack to different components of the power systems can be assessed and used to rank those components in terms of the associated risk. This kind of analysis can be exploited for designing proper defense plans and for allocating scarce budgets to the most convenient defense actions in protecting sensitive targets.

The coordination strategies impact under emergency has been studied with a multiagent system that can effectively simulate the interdependent decision of set of system operators under attacks. It is also proposed to simulate the interactions between different stakeholders of the defender to discover the potential new vulnerability of infrastructure system due to inappropriate coordination. Based on this scenario, simulation of information impacts in the joint defending strategies by multi-agent system is also discussed.

Additional work is underway in different areas. The problem of uncertainty in the information owned both from the attacked and the defender and its impact are

being modelled with a Bayesian game. The impact of information available to the operator under attacks, that may be also cut off as a result of a malicious attack, is being represented in the framework of multiagent system aiming to point out the most critical information that need to be assured with proper actions. Also a proper model and software environment for testing ex-ante different coordination rules among various system operator in the European framework, is being developed with the goal of providing an effective tool to design the most proper coordination rules for managing emergency.

7. REFERENCES

- [1] C.-C. Liu, J. Jung, G. T. Heydt, V. Vittal, and A.G. Phadke, The strategic power infrastructure defense system. a conceptual design, IEEE Control Systems Magazine, 2000, 20(4), pp. 40-52.
- [2] M. Amin, North American Electricity Infrastructure. Are we ready for more perfect storms? IEEE Security and Privacy magazine, 2003, 1(5), pp. 19-25.
- [3] B.J. Garrick, J.E. Hall, M. Kilger, Confronting the risks of terrorism: making the right decisions, Reliability Engineering and System Safety, 2004, 86(2), pp. 129-176.
- [4] E. Bompard, C. Gao, R. Napoli, A. Russo, M. Masera, A. Stefanini, The analysis of malicious threats to power systems: a conceptual approach based on game theory, The International Conference on Dependable Systems and Networks, June 25th-June 28th, 2007, Edinburgh, UK.
- [5] E. Bompard, R. Napoli, A. Russo, F. Xue, M. Masera, A. Stefanini, The analysis of malicious threats to power systems: a conceptual approach based on multi-agent systems, First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, March 19th -21st, 2007, Dartmouth College, Hanover, New Hampshire, USA.
- [6] A.S. Khan, D.L. Swerdlow, D.D. Juranek, Precautions against biological and chemical terrorism directed at food and water supplies, Public Health Reports, 2001, 116(1), pp. 3-14.
- [7] R. Torbin, Urban infrastructure security, Technology in Society, 2003, 25(4), pp. 549-552.
- [8] E.L. Glaeser, J.M. Shapiro, Cities and Warfare: The Impact of Terrorism on Urban Form, Journal of Urban Economics, 2002, 51(2), pp. 205-224.
- [9] <http://www.answers.com/topic/new-york-city-blackout-of-1977>.
- [10] A. Stefanini, Electric System vulnerabilities: Lessons from recent blackouts and the role of ICT, EUR 21551 EN, European Communities, 2005.
- [11] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT, Critical Infrastructure Protection in the fight against terrorism, Brussels, 08/10/2004, COM (2004) Rev 3).
- [12] CRITICAL INFRASTRUCTURE PROTECTION, Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities, United States Government Accountability Office, May 2005 (GAO-05-434).
- [13] K. Siqueira, T. Sandler, Terrorists Versus the Government: Strategic Interaction, Support, and Sponsorship, Journal of Conflict Resolution, 2006, 50(6), pp. 878-898.
- [14] G. Daniel, M. Arce, T. Sandler, Counterterrorism, A Game-Theoretic Analysis, Journal of Conflict Resolution, 2005, 49(2), pp.183-200.

- [15] O. Ercetin, L. Tassiulas, Market-based resource allocation for content delivery in the Internet. *IEEE Transactions on Computers*, 2003, 52(2), pp. 1573–1585.
- [16] M.G.H. Bell, A game theory approach to measuring the performance reliability of transport networks. *Transportation Research Part B: Methodological*, 2000, 34(6), pp. 533–545.
- [17] Z. Yang, A pseudo ‘folk’ theorem in the strategic provision of stock externalities. *International Game Theory Review*, 2003, 5(4), pp. 347.
- [18] E. Bompard, M. Yuchao, E. Ragazzi, Micro-economic analysis of the physical constrained market: game theory application to the competitive electricity markets, *European Physics Journal B*, 2006, 50(1-2), pp. 153-160.
- [19] E. Bompard, W. Lu, R. Napoli, Network constraint impacts on the competitive electricity markets under supply-side strategic bidding, *IEEE Transactions on Power Systems*, 2006, 21(1), pp.160 – 170.
- [20] L.A. García-Cortés, G. Yagüe, C. Moreno, Optimum family size in progeny testing and the theory of games. *Livestock Production Science*, 2000, 64(2-3), pp.193–202.
- [21] J.F. Galloway, Game theory and the law and policy of outer space. *Space Policy*, 2004, 20(2), pp. 87–90.
- [22] J. Neumann & O. Morgenstern, *Theory of Games and Economic Behavior*. Princeton University Press, 1944.
- [23] J.F. Nash, Equilibrium Points in N-Person Games. *Proc Natl Acad Sci U S A*. 1950 January; 36(1): 48–49.
- [24] J. Glazer, A. Rubinstein, An Extensive Game as a Guide for Solving a Normal Game, *Journal of Economic Theory*, 1996, 70(1), pp. 32-42.
- [25] M.B. Stinchcombe, Nash equilibrium and generalized integration for infinite normal form games, *Games and Economic Behavior*, 2005, 50(2), pp. 332-365.
- [26] K. Binmore, J. McCarthy, A Backward Induction Experiment *Journal of Economic Theory* 2002, 104(1), pp. 48-88.
- [27] T. Sandler, J. T. Tschirhart, J. Cauley, A Theoretical Analysis of Transnational Terrorism *The American Political Science Review*, 1983, 77(1), pp. 36-54.
- [28] T. Sandler, G. Daniel, M. Arce, Terrorism & game theory, *Simulation & Gaming*, 2003, 34(3), pp.319-337.
- [29] H.E. Lapan, & T. Sandler, To bargain or not to bargain: That is the question. *American Economic Review*, 1998, 78(2), pp.16-20.
- [30] R. Selten, (1988). A simple game model of kidnappings. In R. Selten (Ed.), *Models of strategic rationality* (pp. 77–93). Boston: Kluwer Academic Press.
- [31] T. Sandler, & H.E. Lapan, The calculus of dissent: An analysis of terrorists’ choice of targets. *Synthese*, 1988, 76(2), pp.245–261.
- [32] T. Sandler, W. Enders, An economic perspective on transnational terrorism, *European Journal of Political Economy*, 2004, 20(2), pp. 301-316.
- [33] O. Berman, A. Gavius, Location of terror response facilities: a game between state and terrorist, *European Journal of Operational Research*, 2007, 177(2), pp.1113-1133.
- [34] G. Daniel, M. Arce. T. Sandler, Counter terrorism- a game theoretic analysis, *Journal of Conflict Resolution*, 2005, 49(2), pp.183-200.
- [35] N. Vlassis, A Concise Introduction to Multiagent Systems and Distributed AI. Online available at: <http://staff.science.uva.nl/~vlassis/cimasdai/cimasdai.pdf>.
- [36] R.S. Sutton & A.G. Barto, *Reinforcement Learning: An Introduction*. MIT Press, Cambridge, MA, 1998 A Bradford Book.
- [37] C. Claus & C. Boutilier, The Dynamics of Reinforcement Learning in Cooperative Multiagent Systems. In:proc. of the Fifteenth National Conf. on Artificial Intelligence,1998

- [38] Union for the Co-ordination of Transmission of Electricity, POLICY 5 EMERGENCY PROCEDURES. UCTE Operation Handbook. Online available at: http://www.ucte.org/pdf/ohb/Policy5_v1.0_03.05.2006.pdf.
- [39] C.B. Excelente-Toledo & N.R. Jennings. Learning When and How to Coordinate. Web Intelligence and Agent System, 1(3-4):203-218, 2003.
- [40] C. Boutilier, Planning, learning and coordination in multiagent decision processes. In Proc. Conf. on Theoretical Aspects of Rationality and Knowledge (1996).
- [41] Y. Shoham and M. Tennenholtz. On the synthesis of useful social laws for artificial agent societies. In Proceedings of the Tenth National Conference on Artificial Intelligence (AAAI-92), pages 276–281, San Jose, California, July 1992.
- [42] E. H. Durfee and V. R. Lesser. Partial global planning: A coordination framework for distributed hypothesis formation. IEEE Transactions on Systems, Man, and Cybernetics, 21(5):1167–1183, September 1991.
- [43] L. Hogg and N. R. Jennings. Socially rational agents. In Proc. of AAAI Fall symposium on Socially Intelligent Agents, pages 61–63, 1997.
- [44] O. I. Elgerd, Electric energy systems theory, An introduction. McGraw-Hill Education - Europe (1998).
- [45] C. Watkins, P. Dayan; Technical Note Q,-Learning. Machine Learning, 8, 279-292 (1992)
- [46] S. Sen, M. Sekaran, & J. Hale. Learning to coordinate without sharing information. In Proceedings of the Twelfth National Conference on Artificial Intelligence, pages 426–431, Seattle, W A, 1994.

8. APPENDIX

Abbreviation

ICT	Information and Communication Technologies
GDP	Gross Domestic Product
EMS	Energy Management System
GT	Game Theory
MAS	Multi Agent System
SO	System Operator
AI	Artificial Intelligence
RL	Reinforcement learning
WoLF	Win or Learn Fast
UCTE	Union for the Co-ordination of Transmission of Electricity

Notation for Game Theory model (5.1)

\mathcal{T}	set of attack actions containing the action toward multiple components simultaneously
a_k^t	k -th action in the attack action set, it contains multiple components to be attacked
\mathcal{F}	set of defense actions containing the action toward multiple components simultaneously
a_k^f	k -th action in the defense action set, it contains multiple components to be defended
B_D	equivalent defense budget for measuring the defense resources
B_A	equivalent attack budget for measuring the attack resources
C_k^A	cost of the attacker for implementing the attack action a_k^t
C_k^D	cost of the defender for implementing the defense action a_k^f
C_i^a	cost of attacking the component i
C_i^d	cost of defending the component i
S_A	payoff of the attacker
S_D	payoff of the defender
C_A	cost of the attacker to perform an attack action
C_D	cost of the defender to perform a defence action,
L_D	economic value of a loss of load
γ_j	equivalent economic value of the load at bus j
ΔD_j	load reduction at bus j
n	number of buses in the network
\mathbf{B}	nodal admittance matrix, $\dim(\mathbf{B}) = n \times n$
$\underline{\theta}$	vector of bus angle, $\dim(\underline{\theta})=n$
\underline{P}	vector of bus power injection, $\dim(\underline{P})=n$
ΔD_j	demand variation at bus j
D_j	demand at bus j , before the attack
g_j	original generated power at the bus j
Δg_j	original generated power and the generation variation at the node j
g_{jmax}	original generated power and the generation variation at the node j .
f_l	line flow in line l
F_l^{max}	line flow limit of the line l
n_l	number of lines in the network
S_A^k	payoff of the attack in the k -th scenario

S_D^k :	payoff of the defender in the k -th scenario
C_A^j :	cost expressed in monetary value of the attacker for implementing attack action j
C_D^i :	cost expressed in monetary value to the defender for implementing defense action i
L_D^k :	loss caused by the power system failure in the k -th scenario
O_i :	i -th component to be considered as the attack/defense target
p_k^A :	probability for the attacker to take the attack action a_k^t
p_i^a :	probability of the component O_i to be attacked
$\underline{\alpha}$:	successful destroy probability vector of the attack without the corresponding defense action taken
$\underline{\beta}$:	successful destroy probability vector of the attack with the corresponding defense action taken
nc :	number of the component considered to be attacked

Notation for MAS model (5.2)

α :	action performed by agent i
U_i^E :	expected utility of agent i by performing α
U_i^I :	individual utility of agent i by performing α
U_i^S :	social utility afforded to the overall system when α is executed
λ^i :	vector of social relationships of agent i
λ_n^i :	social relationship of agent i with agent n
φ^i :	vector of coefficient that weight the importance of those relationships in λ^i
φ_n^i :	coefficient that weight the importance of relationship with agent n
$U_j^S(\alpha)$:	social relationship utility, the utility afforded to the agent in λ_j^i by the execution of α
k_1 :	coefficient devoted to weight the individual utility on the expected utility of an action α
k_2 :	coefficient devoted to weight the social utility on the expected utility of an action α
A :	action scheme which consists of the possible control actions
$Q(s, \alpha)$:	Q value for action α at state s
R_i :	reward for agent i
β :	updating rate
L :	set of all lines
P^l :	power flow on line l
P_{max}^l :	maximum power limit of line l
U^l :	utility of line l
I_i :	set of internal lines for agent i
T_i :	set of tie-lines for agent i
P_k^i :	sum of absolute values of power flow at all tie-lines between agent i and agent k
M :	constant number, bigger than the sum of loads possible to be shed in one action scheme
$Load_i$:	sum of loads shed by agent i in the local subsystem in the implemented action scheme
$p.u.$:	per unit

European Commission

EUR 22683 EN – DG Joint Research Centre, Institute IPSC

Title: APPROACHES TO THE SECURITY ANALYSIS OF POWER SYSTEMS: DEFENCE STRATEGIES
AGAINST MALICIOUS THREATS

Authors: **E. Bompard, C. Gao, M. Masera, R. Napoli, A. Russo, A. Stefanini, F. Xue**

Luxembourg: Office for Official Publications of the European Communities

2007 – 51 pp.

EUR - Scientific and Technical Research series; ISSN 1018-5593

Abstract

This report is intended to provide a conceptual framework for assessing the security risk to power systems assets and operations related to malicious attacks. The problem is analysed with reference to all the actors involved and the possible targets. The specific nature of the malicious attacks is discussed and representations in terms of strategic interaction are proposed. Models based on Game Theory and Multi Agent Systems techniques specifically developed for the representation of malicious attacks against power systems are presented and illustrated with reference to applications to small-scale test systems.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.